IDA

I N S T I T U T E   F O R   D E F E N S E   A N A L Y S E S

Open Scenario Study, Phase II Report: Assessment and Development of Approaches for Satisfying Unclassified Scenario Needs

Jason A. Dechant, Study Co-Lead
James S. Thomason, Study Co-Lead
Ylli Bajraktari
Mary Catherine Flythe
Anthony C. Hermes
Nicholas S. J. Karvonides
Michael F. Niles
Zachary S. Rabold
Robert T. Raffel

Contributor
Rachel Dubin

The Institute for Defense Analyses is a non-profit corporation that administers three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-4537

Open Scenario Study, Phase II Report: Assessment and Development of Approaches for Satisfying Unclassified Scenario Needs

Jason A. Dechant, Study Co-Lead
James S. Thomason, Study Co-Lead
Ylli Bajraktari
Mary Catherine Flythe
Anthony C. Hermes
Nicholas S. J. Karvonides
Michael F. Niles
Zachary S. Rabold
Robert T. Raffel

Contributor
Rachel Dubin

PREFACE

This document reports the work performed by the Institute for Defense Analyses in partial fulfillment of the task order titled "Open Scenarios for Defense Planning." The work was sponsored by the Modeling and Simulation Coordination Office (MSCO), Office of the Deputy Under Secretary of Defense for Science and Technology with additional oversight by the Office of the Director Cost Assessment and Program Evaluation and the Force Structure, Resources, and Assessment Directorate (Joint Staff, J8). The authors wish to thank the reviewers, Dr. Michael Fitzsimmons, Dr. Vance Gordon, and Mr. Fred Hartman of the Institute for Defense Analyses, and Ms. ElizaBeth Johnson for editing the document. All trademarks are the property of their respective owners.

CONTENTS

APPENDICES

FIGURES

SUMMARY

The Department of Defense (DoD) requested the Institute for Defense Analyses (IDA) assess the national security community's needs for unclassified (or "open") scenarios and evaluate approaches for satisfying those needs. For this reason, IDA initiated the Open Scenario Study. Phase One of the study found that a significant demand for unclassified scenarios exists, that there are large recurring costs associated with scenario development, and that options for major cost-savings exist.[1]

In Phase One of the Open Scenario Study, IDA identified methods DoD might use to address the demand for unclassified scenarios. These methods can be translated into four major "elements" that any DoD approach to meeting unclassified scenario demand could include:

Element One – an online open scenario repository,

Element Two – the certification of existing unclassified scenarios,

Element Three – development of new unclassified scenarios, and

Element Four – the declassification of classified scenarios.

In Phase Two of the study, IDA examined these four elements independently and in combination. Ultimately, IDA determined the national security community's demand for unclassified scenarios could best be met by using a combination of several of the elements. This report highlights major findings from Phase Two and offers IDA's recommended approach for better addressing DoD's need for unclassified scenarios.

BACKGROUND

Phase One of the Open Scenario Study showed that unclassified scenarios are used throughout DoD and serve a variety of functions. While DoD has a codified and institutionalized process for the development of a common set of classified scenarios, no

---

[1] A detailed summary of Phase One and its major findings appear in Appendix A of this report. The complete results of Phase One are documented in *Open Scenario Study, Phase I: Assessment Overview and Results,* (IDA Paper P-4326), by Jason A. Dechant and James S. Thomason et al., Institute for Defense Analyses, March 2008.

such process exists for the development of unclassified scenarios.[2] Consequently, those who develop and use unclassified scenarios have undertaken disparate efforts that have frequently produced redundant unclassified scenarios. To offer potential solutions to better address the need for unclassified scenarios and reduce associated development costs, DoD asked IDA to design an approach that may be used in the Department and with its partners.

PHASE TWO METHODOLOGY

The overall Open Scenario Study design includes two phases: Phase One-assessment of unclassified scenario demand and Phase Two, development and assessment of approaches for satisfying the demand, and recommendations for implementation. This report conveys the results of Phase Two.

During IDA's assessment of the demand for unclassified scenarios in Phase One, the unclassified scenario user community provided perspectives on how it uses scenarios and how the processes for developing and sharing unclassified scenarios might be improved. These perspectives highlighted how unclassified scenario "user communities" can be loosely aggregated according to their organization's functions.[3]

In Phase Two of the study, IDA translated methods, identified in Phase One, that could potentially satisfy the existing demand for unclassified scenarios into four distinct "elements." Furthermore, Phase Two evaluated these elements, both independent of one another and in combination.

The first part of Phase Two involved scrutinizing each of the elements individually, exploring potential variations in their design as well as detailed descriptions of what each element would entail. Additionally, this part included analyzing each of these elements to determine their potential benefits and limitations and assessing their likely effectiveness in helping satisfy existing and future demand for unclassified scenarios. In the second part of Phase Two, the IDA study team considered combinations

---

[2] DoD maintains a library of Defense Planning Scenarios (DPS) which make up its official classified scenario set. DPSs are developed through a codified, institutionalized process within the Department's Analytic Agenda framework. For additional discussion on DPSs and the Analytic Agenda, see Appendix B of this report.

[3] In the Phase One report, each of the following functions also loosely represents a scenario user community: force structure and capability mix analysis; acquisition; concept development and experimentation; wargaming; training and education; testing; intelligence and threat assessment; and operational planning. See *Open Scenario Study, Phase I: Assessment Overview and Results* (IDA Paper P-4326), p. 26.

of the elements that might be used to construct an approach. Approaches were assessed with careful consideration of three selection criteria. Selection criteria included:

- Availability: availability of the approach, and its contents, to the largest possible audience of unclassified scenario users,

- Flexibility: ease with which changes in scenario content can be made available to the community of unclassified scenario users, and

- Responsiveness: responsiveness to the varying aspects of unclassified scenario users' demand for unclassified scenarios.

MAJOR FINDINGS

Phase Two analysis yielded several major findings:

1. **Few, if any, organizations have awareness of and access to the universe of unclassified scenarios developed and used by DoD and its interagency partners.** One of the main impediments in meeting the demand for unclassified scenarios is awareness and accessibility. The development and employment of a new approach would make existing unclassified scenarios available to those who need them, and help to meet unclassified scenario demand.

2. **DOD would benefit from promoting the reusability of unclassified scenarios.** Today, the development of unclassified scenarios is not based on integrated, DoD-wide processes, is not widely shared or coordinated among the Department's diverse base of users and interagency partners, and does not encourage the widespread distribution of the final scenario product, all resulting in redundancy. The reuse and greater sharing of existing scenarios could reduce unnecessary duplication of effort, help save costs, increase DoD-wide knowledge sharing and develop best practices, and improve interagency collaboration and coordination.

3. **The U.S. Army's unclassified Multi-Level Scenario (MLS) framework provides a potential foundation for joint unclassified scenarios development and use.** Within DoD, the U.S. Army's Multi-Level Scenario (MLS) provides an example of an existing codified and institutionalized process that could be utilized and leveraged while developing a new

approach.[4] The MLS is used for modeling and simulation and is tailored to meet customers' needs.

4. **Unclassified scenario development and use provide a unique opportunity to strengthen interagency collaboration and coordination.** Both civilian and military agencies use scenarios for exercises and planning efforts, but there are few common platforms that create appropriate and open linkages. The development and employment of an approach that provides unclassified scenarios to disparate government agencies would encourage interagency collaboration and "whole-of-government" coordination.

IDA'S RECOMMENDED APPROACH

Based on the significant demand for unclassified scenarios that was identified in Phase One of the Open Scenario Study and the major findings of Phase Two, IDA proposes that DoD adopt the following approach:

Certify selected existing unclassified scenarios (for example the Army's MLS 1.0 and 2.0) (Element Two) based on the preferences of the individual unclassified scenario user communities identified in Phase One, and develop new unclassified scenarios as needed through a distributed development model (Element Three) to create an official set(s) of unclassified scenarios. These scenarios and other existing unclassified scenarios should be housed in an online repository (Element One). (Details of the online repository are provided in Chapter II.)

IDA recommends the online open scenario repository include the following key features:

1. The repository should be a summary database with basic query capability that enables keyword and Boolean search queries and is equipped with an "advanced search" function that allows users to type in more than one specific search term and search within specific fields.

2. Equip the repository with a wiki engine that would allow users to post new or edited scenarios to the repository, provide feedback on scenarios, and rate scenarios according to their utility for a given function.

---

4 A detailed summary and major findings appear in Appendix E of this report. For a more complete description of the U.S. Army's MLS, see *Open Scenario Study: U.S. Army's Multi-Level Scenario Sub-Task* (IDA Paper P-4466), by Jason A. Dechant and James S. Thomason et al., Institute for Defense Analyses, July 2009.

3. Include a blog that allows the repository's managers to post news and updates, a feedback form that allows repository users to comment directly and anonymously to the repository managers, and a message board that enables discussion between repository users and possibly stimulate future collaboration among users.

4. Grant access to the repository's content by grouping scenarios into different categories based on each scenario's classification. The first category of scenarios would include scenarios that are unclassified and approved for public release. The second category of scenarios would require users to demonstrate a "need-to-know" their content. The third category of scenarios would include scenarios that have specific developer/owner-defined special restrictions and access.

5. As information to users, the repository should note which, if any, scenario components a given scenario has and its level of detail.[5]

6. The online repository should be housed on an official DoD website and owned by a joint organization that is expanded to include the DoD's key interagency partners who have a demonstrated interest in the direction and content of the repository. The organization would provide top-level strategic guidance to the repository's day-to-day managers and have control over its budget.

7. Communities of unclassified scenario users should be required to define their community's overall scenario needs and preferences. They should advise the designated joint parent organization regarding scenarios important to their activities that must be promulgated, either through the certification of existing scenarios or the development of new unclassified scenarios, and that should also be included in the repository.

IDA's recommended approach is derived from a combination of three (of four) individual elements described and evaluated in Chapters II. through V. of this report:

Element One – an online repository that houses official sets of unclassified scenarios;

Element Two – the certification of existing unclassified scenarios;

---

5   Example components include: assumptions, context/road to war, threat/challenge, objectives, strategic concept, concept of operations, and forces data.

Element Three – the development of new unclassified scenarios, as needed.

Element Four – the declassification of the classified scenarios was considered, but this element was excluded from the recommended approach because declassified scenarios may lose their value after being sanitized of classified information and the identification of appropriate replacement information and sources would be difficult.[6]

IDA also examined the possibility of each of the elements serving as a standalone approach for meeting existing demand for unclassified scenarios. However, none of the elements performed well enough against the selection criteria to serve as a standalone component of an approach.

The success of this approach is highly contingent upon the involvement of relevant senior managers in DoD and their willingness to incur real costs, both financial and human, in the implementation, construction, and maintenance of IDA's recommended approach.[7] Absent strong support from DoD's leadership and the allocation of appropriate resources, the effectiveness of the approach would be hindered and the demand for unclassified scenarios unmet.

This report also includes seven appendices, which contain summaries, methodologies, and research methods that IDA relied on to prepare the report. These appendices will provide greater insight regarding IDA's recommended approach.

Appendix A summarizes the Open Scenario Phase One's major findings.

Appendix B summarizes DoD's Analytic Agenda process.

Appendix C is a taxonomy of potential fields that may be used to search/browse an online open scenario repository.

Appendix D highlights IDA's dialogue with Allied and Interagency organizations regarding Phase Two of the Open Scenario Study.

Appendix E summarizes the U.S. Army's Multi-Level Scenario (MLS) Sub-Task report.

Appendix F provides a graphic depiction of the approaches evaluated by IDA in Phase Two and IDA's recommended approach.

---

6   IDA's government sponsors also eliminated declassification as a potential element of an approach.

7   The offices of relevant senior managers are identified in subsequent chapters of this report.

Appendix G highlights several major technical considerations for building an online open scenario repository.

Additionally, the accompanying compact disc (CD) includes Volumes I-III of the Phase One Report, titled *Open Scenario Study: Phase I: Assessment Overview and Results*, (IDA Paper P-4326), and the most current beta version of IDA's Open Scenario Repository.[8]

---

[8] Use of the beta repository requires Microsoft Access®. The *IDA Open Repository Beta Site* can be accessed at http://openscenarios.ida.org/. IDA does not make a recommendation regarding specific software to be used for the repository, but rather uses Microsoft Access® for demonstrative purposes.

I.   INTRODUCTION

The Department of Defense (DoD) asked the Institute for Defense Analyses (IDA) to assess the national security community's need for unclassified scenarios and develop approaches for satisfying the identified need. Phase One of the Open Scenario Study found that a significant demand exists.[1] IDA also found that the recurring costs for scenario development are excessive but potential options for major cost-savings exist and should be further explored.

Additionally, Phase One of the Open Scenario Study revealed a number of user preferences and insights into the characteristics of an approach for satisfying the community's need for unclassified scenarios. These preferences were not always consistent and they were often specific to particular user groups. However, they could be collectively aggregated and characterized by four basic elements of an approach to better satisfy the need for unclassified scenarios:

> **Element One - Online Repository –** An online, searchable database of unclassified scenarios developed by any available sources.

> **Element Two - Certification of Existing Scenarios –** Designation of a pre-existing set of unclassified scenarios, developed by any source, as "preferred" for use throughout the national security community.

> **Element Three - Development of a New Unclassified Scenario Set –** Development and maintenance of a new set of unclassified scenarios akin to classified Defense Planning Scenarios (DPSs).[2]

---

[1] The complete results of Phase One are documented in *Open Scenario Study, Phase I: Assessment Overview and Results* (IDA Paper P-4326), by Jason A. Dechant and James S. Thomason et al., Institute for Defense Analyses, March 2008.

[2] The Defense Planning Scenarios (DPS) are part of the Secretary's guidance to DoD on capabilities development planning and programming. Each DPS depicts a specific hypothetical operational challenge that might be faced by the future force. Together, all DPSs are meant to address a full range of major military operations. DPS are produced for two future timeframes, nominally the "mid-term" (Future Year Defense Program +1) and the "long-range" (Future Year Defense Program +13). See Appendix B of this report and *Improving Integration of Department of Defense Processes for Capabilities Development Planning* (IDA Paper P-4154), by Daniel Cuda, et al., September 2006, C-1.

Element Four - Declassification of Classified Scenarios – Identification and removal of sensitive material in classified scenarios to produce an official, unclassified set.

A. PHASE TWO METHODOLOGY

IDA pursued a two-part methodology to systematically examine each of the four elements that could be used to meet the national security community's demand for unclassified scenarios. First, the IDA study team scrutinized each of the elements individually and independent of one another and prepared four white papers that are featured in Chapters II. through V. of this report.

Selection Criteria

The second part of the Phase Two methodology involved examining approaches that used each of the four elements as a stand-alone solution and in combination with one another. These approaches were evaluated by members of the IDA study team with careful consideration of three selection criteria:

- Availability: availability of the approach, and its contents, to the largest possible audience of unclassified scenario users,

- Flexibility: ease with which changes in scenario content can be made available to the community of unclassified scenario users, and

- Responsiveness: responsiveness to the varying aspects of unclassified scenario users' demand for unclassified scenarios.

These criteria were chosen for several reasons. First, it is logical to assume that any approach that can be made available to the largest audience of unclassified scenarios users as attainable is *most likely* to satisfy the largest possible amount of the identified demand for unclassified scenarios.

Second, during Phase One, IDA became aware of the fact that many organizations, both inside and outside DoD, develop unclassified scenarios on an ad hoc basis, for example the Army's MLS 1.0 and 2.0. The scenarios developed in decentralized, intra-organizational processes may be useful to other organizations in the broader community of unclassified scenario users, but may not be accessible to those who would use them. Therefore, an approach should also be conducive to sharing dynamic scenario content throughout the community of unclassified scenario users.

Finally, in Phase One IDA learned that unclassified scenario users had different types of demand for unclassified scenarios. While some users' demand may be satisfied by using any number of unclassified scenarios, others may require scenarios with official standing in their user community. Therefore, any deployed approach must also be responsive to the varying aspects of unclassified scenario users' demand for scenarios.

Through interactions with the project's government sponsors IDA determined that there is a strong preference in both the unclassified scenario developer and user communities for an open online repository of unclassified scenarios. In large part this preference was based on the assessment that a repository would be available to the widest audience of unclassified scenario users, and would satisfy a great deal of unclassified scenario demand

IDA also discerned that the declassification of classified DPSs and vignettes should not be included in an approach aimed at meeting the national security community's demand for unclassified scenarios.[3]

Potential Approaches

In response to these preferences, IDA specifically designed, analyzed, and evaluated four different approaches, all of which include "Element One" (the repository) and none of which include "Element Four" (declassification):

1. **Create Open Scenario Repository** – House or link existing unclassified scenarios, developed by any available sources, in a searchable, online virtual space (Element One only).

2. **Certify and House Existing Unclassified Scenarios in a Repository** – Certify existing unclassified scenarios to create an official set of unclassified scenarios that is housed in an online repository (Elements One and Two).

3. **House Newly Developed Scenarios in a Repository** – Develop a new, official set of unclassified scenarios and house them in an online repository (Elements One and Three).

4. **Certify Existing and Develop New Unclassified Scenarios and House in a Repository** – Certify existing unclassified scenarios and develop new unclassified scenarios to create an official set of unclassified scenarios that is housed in an online repository (Elements One, Two, and Three).

---

[3] For further explanation, see Chapter V of this report.

Each of the elements was also considered as a standalone approach but for reasons discussed in Chapters II. through V. the standalone approach was not viable.

B. U.S. ARMY'S MULTI-LEVEL SCENARIO SUB-STUDY

In reviewing the universe of existing unclassified scenarios sets and development processes that could be used, IDA became aware of the U.S. Army's unclassified Multi-Level Scenarios (MLS) approach. The primary purpose of the MLS is to provide a set of unclassified scenarios that supplement DoD's classified scenarios and provide an unclassified analytic space for assessing Joint Land Operations across a range of military operations and with the participation of civilian agencies and foreign partners. Subsequently, members of the IDA study team performed a sub-study that examined the Army's need for, development, and use of the MLSs. Ultimately, IDA concluded the Army's MLS development process *could* serve a number of DoD/Joint purposes if other Service and defense organizations are included in the MLS development process and the scenarios should be made more widely available for use by the universe of unclassified scenario users.[4] Included in Chapter III. is a more detailed discussion regarding the Army's MLS scenario suite, development process, and its potential application towards an approach for meeting existing demand for unclassified scenarios.

C. ALLIED AND INTERAGENCY COLLABORATION

In Phase One of the study IDA analyzed reasons why DoD might have a demand for unclassified scenarios. During this effort the study team determined that a significant driver behind the demand for unclassified scenarios was the Department's necessity to include its interagency partners and foreign allies in a variety of functions that use scenarios. In large part, the necessity of "whole-of-government" collaboration, which includes DoD and its interagency partners, is driven by an increasingly common civil-military challenge space. Success in this challenge space is often defined by collaboration and cooperation between civilian and military organizations, both foreign and domestic, across a broad range of contingency and planning efforts, to include conventional, irregular warfare, counterinsurgency operations (e.g., Operation Enduring Freedom in Afghanistan), and domestic disaster relief (e.g., Hurricane Katrina). To avoid difficulties that arise from the use of classified scenarios, such as prohibiting participation of those

---

[4] For a more complete description of the Army's MLS, see *Open Scenario Study: U.S. Army's Multi-Level Scenario Sub-Task* (IDA Paper P-4466), by Jason A. Dechant and James S. Thomason et al., Institute for Defense Analyses, July 2009.

without a security clearance, often unclassified scenarios are the preferred *modus operandi*.

In order to ensure a consistent and holistic approach to Phase Two of the study, IDA continued to expand its dialogue with various DoD partner organizations including the Department of State (DoS) and the Department of Homeland Security (DHS). IDA solicited feedback from these organizations throughout Phase Two in order to gain a broader perspective on how an approach might serve as a platform that could help foster collaboration between DoD and its partner organizations, as well as expose both military and civilian stakeholders to a collection of challenging and new unclassified scenario sets.[5]

D. ORGANIZATION OF PHASE TWO REPORT

Chapters II. through V. introduce each of the aforementioned four individual elements of an approach and examine them independent of one another.

Chapter VI. details IDA's recommended approach and describe its functional design, management, and ownership processes.

Chapter VII. summarizes the major Phase Two findings and highlights future considerations that must be addressed before the recommended approach is implemented.

Also included in this report are seven appendices, which contain summaries, methodologies, and research methods that IDA relied on to prepare this report. These appendices will provide greater insight regarding IDA's recommended approach.

Appendix A summarizes the Open Scenario Phase One's major findings.

Appendix B summarizes the Analytic Agenda process.

Appendix C is a taxonomy of potential fields that may be used to search/browse an online open scenario repository.

Appendix D highlights IDA's dialogue with Allied and Interagency organizations regarding Phase Two of the Open Scenario Study.

Appendix E summarizes the U.S. Army's Multi-Level Scenario (MLS) Sub-Task report.

---

[5] For a more descriptive account of IDA's interaction with non-DoD organizations during Phase Two, see Appendix D of this report.

Appendix F provides a graphic depiction of the approaches evaluated by IDA in Phase Two and IDA's recommended approach.

Appendix G highlights several major technical considerations for building an online open scenario repository.

II. ELEMENT ONE: ONLINE OPEN SCENARIO REPOSITORY

As indicated earlier in this report, the central feature of the repository will be its open online functionality (Element One). The main purpose of this element is to provide a library of unclassified scenarios in a widely accessible virtual space to those who need them. This chapter outlines some of the key considerations and features that could be included in an online open scenario repository.

A. DESCRIPTION OF THE ELEMENT

There are many different considerations relevant to building an online open scenario repository.

1. What are the standards for access by users?

2. What standards must a scenario meet in order to be included in the repository?

3. What organization structure and management scheme is used to operate the repository?

4. How do users locate scenarios within the repository?

5. How does the repository direct users to unclassified scenarios?

6. Is there a rating system that determines how useful scenarios are?

7. How do the repository's owners/managers and users communicate and collaborate with one another (e.g., announcements, updates, questions, etc.)?

The purpose of this chapter is to explore answers to these questions and discuss variables that could be used to structure an online open scenario repository.

1. What are the standards for access by users?

a. Degrees of Access

A repository would have a relationship with three groups of people: owners (those who are responsible for the repository), managers (those who run the repository on a day-to-day basis), and users (those who use the repository's resources). The owners and

managers of the repository would be responsible for many key functions, such as granting users access to the repository. While an online open scenario repository may have varying degrees of access, the repository's owners and/or managers would be responsible for developing standards for gaining access to the repository's scenarios. (See Section b for more discussion on standards for access.) Across the spectrum, each degree of access has a different level of exclusivity regarding who may and may not have access to the repository, with "open" being the degree that is *least* exclusive and "restricted" being the degree that is *most* exclusive (See Figure 1. below).
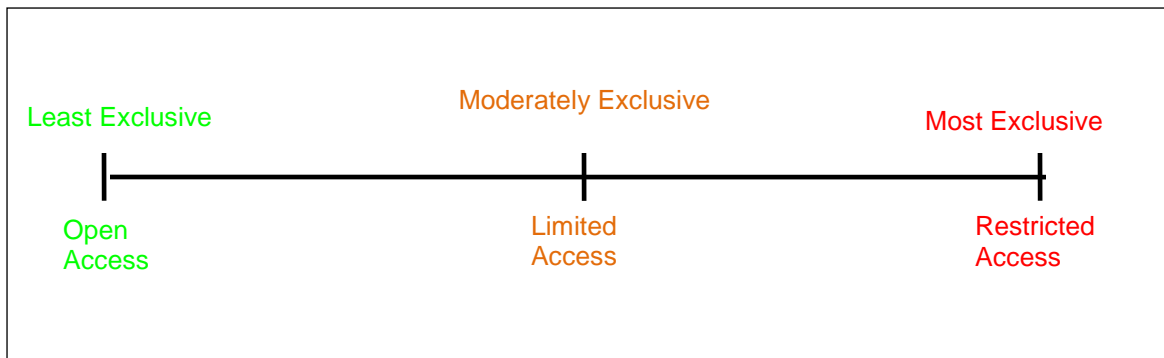
Figure 1. Different Level of Access

The least exclusive degree of access for an online open scenario repository is "open" access. An open access repository would allow virtually anyone, including the entire community of unclassified scenario developers and users, to use the scenarios housed in the repository regardless of their affiliation to DoD. An example of a virtual DoD entity with open access is the website www.Defenselink.mil/pubs/, which makes current unclassified DoD publications available to any individual or organization with Internet access.

The moderately exclusive degree of access for an online open scenario repository would be a repository with "limited" access. A limited access repository would grant more access than a "restricted" repository, but would not be entirely open to the community of unclassified scenario developers and users or any individual or organization with internet access. A limited access repository would require the development of access standards that can be applied to a screening process for granting access. Examples of limited access online DoD resources are the Modeling and Simulation Resource Repository (MSRR) and Defense Technical Information Center

(DTIC) library which, despite being available on the internet, require potential users to meet the standards of a screening process before becoming a user of either repository.

The most exclusive degree of access for an online open scenario repository would be a "restricted" access repository that would grant access to a select group of individuals or organizations within or closely associated with DoD. A restricted access repository would require the rigorous application of access standards in a screening process and could potentially exclude a large portion of the community of unclassified scenario developers and users. An example of a restricted access online DoD resource is E-Room, which requires a Common Access Card (CAC) and is not available in the public domain.

Despite the differing exclusivity each degree of access implies, they are not mutually exclusive in that they could all be used within the same overall repository. It is possible that an online open scenario repository has "layered" access, in which certain unclassified scenarios are available to the entire community of unclassified scenario developers and users (open access), while other scenarios (for example, those classified as For Official Use Only (FOUO)) are available to only a select few. Therefore, an online open scenario repository with layered access would be largely contingent upon the classifications and types of scenarios it houses.

b. Standards for Access

The judgment of how accessible an online open scenario repository should be is a decision that would be made by the repository's owners. The repository's owners would first have to decide how much of the demand for unclassified scenarios they wish to meet and how secure they wish the repository's scenarios to remain, both of which would determine how much access is granted. Subsequently, they would develop a set of standards to fit the desired level of access. Some potential standards for access include:

- affiliation with DoD (e.g., employee, government partner, contractor, anyone, etc.)

- intended use of scenarios (e.g., providing a task number or statement of purpose)

- "need-to-know"

With each additional standard for access, and the degree of intensity with which they are applied, the repository's owners would be making a judgment on how exclusive the repository is. For example, if the owners decided to grant open access to the repository, they may have no standards for access, or simply have a few (e.g., name,

organization, contact information, etc.) for administrative, demographic, and identification purposes. If the owners want a highly restricted repository, they may rigidly apply numerous standards of access to potential users, which limits who gains access to the repository's resources.

2. What standards must a scenario meet in order to be included in the repository?

Similar to developing standards for user access, the repository's owners will also need to develop a list of criteria that determine which scenarios are included in the repository's set, so as not to include documents that are not scenarios. Several criteria that could be used to determine a scenario's inclusion are:

- the document must be written in English;

- A common, agreed-upon definition is used to screen whether documents are scenarios and thus warrant inclusion;[6]

- the decision that only scenarios with certain components will be included in the repository;[7]

- the developer or sponsor of the scenario is approved (e.g. an official DoD scenario vs. John Doe's scenarios);

- military vs. non-military orientation (e.g., scenarios that depict major combat operations vs. scenarios that depict famine).

There are also varying degrees of scrutiny that can be applied to these standards. Since the standards for including a scenario in the repository are likely to be subjective, they can be applied loosely or strictly, which will determine how many scenarios are

---

[6] Phase One of the Open Scenario study found that no official definition of scenario exists within DoD. However, the questionnaire indicated that seventy-eight percent of respondents agreed that a scenario could generally be defined as "depictions of a threat to international security, a corresponding mission for U.S. and allied capabilities, and a strategic concept for carrying out that mission." This paper does not advocate that this specific definition be used as a screening mechanism for scenario inclusion; instead, the paper offers the definition as an example of one that could be used to determine a scenario's inclusion. See *Open Scenario Study, Phase I: Assessment Overview and Results* (IDA Paper P-4326).

[7] Ibid. Phase One of the Open Scenario study found that nearly all questionnaire respondents agreed that the following components were important to the structure of a scenario: assumptions, context/road to war, threat/challenge, objectives, strategic concept, concept of operations, and forces data. This paper does not advocate that all of these specific components be used as a screening mechanism for scenario inclusion; instead, the paper offers them as examples of components that could be used to determine a scenario's inclusion in the repository.

included in the repository and their quality (e.g., highly refined, formal scenario products vs. "rough sketch" scenarios).

Additionally, the repository owners and/or managers would also be responsible for promulgating the initial library of scenarios included in the repository. This would likely require the repository's owners and managers to be granted authority, possibly by a DoD Instruction, to obtain unclassified libraries of scenarios developed by various DoD offices.

3. What organization and management scheme is used to operate the repository?

As with any other repository or database, an online open scenario repository would need a management system that controls access, updates the repository, etc. The system of management that is used to run the repository is contingent upon how robust the owners want the repository to be used and how many scenarios it houses. If the repository is populated with a large number of scenarios and has many of the features discussed in this report (e.g., physically contains the scenarios, has limited or restricted access, has a blog and/or message board, a specific rating system, etc.) then it will likely be more labor-intensive to support the repository (more management staff, time, money, etc.). Conversely, if the owners choose to run a smaller repository with very few of the features discussed in this report then it will likely need a less extensive support infrastructure.

No matter how little labor the management system of the repository requires, the managers will be required to perform certain necessary functions. Some of these functions include (options appearing below are discussed in-depth in subsequent sections of this chapter):

- reviewing applications for and granting access to persons or organizations (unless it is an open repository),
- updating the repository with new scenarios,
- filling out the taxonomy of searchable fields for each scenario,
- providing ratings to scenarios (or manage user ratings, if applicable),
- screening user comments on scenarios,
- issuing updates (on a blog and/or message board, if applicable), and
- deciding whether potential new scenarios are qualified for inclusion.

In a robust repository with more features, support functions will also be required to:

- police and moderate the message board,

- run anti-virus scans of new scenarios (in a repository that makes scenarios available for download),

- format new scenarios (in a repository that makes scenarios available for download),

- link users to scenarios and maintain current links (in a repository that links users to secondary sources), and

- be receptive to feedback from users.

Ultimately the repository's system of management will rely on the structure of the repository and how many features it has. While many basic management functions will be performed by the repository's managers regardless of how robust the repository is, many other management functions are dictated by any additional variables the repository's owners prefer.

4. How do users locate scenarios within the repository?

Because of the high likelihood that a very large number, perhaps thousands, of scenarios would be housed in an online open scenario repository, the ability to easily search and/or browse the repository's content would be a key feature of its interface. Just as online resources such as Google, JSTOR, and Lexis-Nexis allow users to sort millions (or in some cases billions) of bits of information into smaller, more relevant lists of information, an online open scenario repository should also allow its users to refine a large set of scenarios into a smaller, more relevant list of scenarios.

With a search function, repository users could enter any relevant keyword into a search bar, allowing a search engine to scan the set of unclassified scenarios and pull up relevant hits. Additionally, the repository's search function may also have Boolean search capability, which would allow users to search through the set of unclassified scenarios using multiple keywords.[8] This basic function would be one of the most useful and important features of an online open scenario repository since it would make

---

[8] Boolean searching is searching done based on the logical relationship among keywords. The three logical operators in Boolean searches are typically: *or*, *and*, and *not*.

identifying scenarios relevant to an individual's needs a relatively simple and familiar task.

A similar, yet different, style of searching the repository could be done if the repository contains a taxonomy of searchable fields, which would let users browse the repository's set of scenarios.[9]   For example, if one of the fields used to search the repository is "Military Operations Depicted," a drop-down menu could be used to make a selection of the military operation that the user is interested in (e.g., major combat operations), which would allow the user to browse every scenario in the repository that depicts major combat operations. To further narrow the choices of scenarios listed from a search, drop-down menus would be available for all fields so that smaller, more relevant lists of scenarios can be browsed if desired or Boolean searches of each field could be conducted by an advanced search feature.

5. How does the repository direct users to unclassified scenarios?

An online open scenario repository could distribute scenarios by either making them available for download or linking users to a secondary source that has the scenarios. While either option is feasible, each has a different set of considerations that must be evaluated.

If a repository is going to make unclassified scenarios available for download, considerations must be given to how much computer memory the repository will have available, especially if the number of scenarios the repository holds continues to grow over time.   In order to maximize the repository's memory capacity, it may be beneficial to set all the scenarios in the repository into a common format (e.g., Adobe PDF file). Additionally, a repository that enables users to download scenarios would need anti-virus protection since it is likely that the repository will be populated from outside sources and the repository's owners and/managers would not want to be responsible for users downloading a contaminated file.

The second method that could direct users to scenarios is to link scenarios on a list to a secondary source that contains the unclassified scenarios. This option requires fewer considerations. Gone are concerns about memory capacity and viruses since scenarios would not be housed directly in the repository and users would download files from outside the repository's virtual space. However, since not all unclassified scenarios

---

9   For a potential taxonomy of fields see Appendix C of this report.

are available on the Internet, linking to scenarios instead of allowing users to download them would severely limit the number of scenarios the repository could direct users to and would require periodic checking of whether the links still function.

6. Is there a rating system that determines how useful scenarios are?

Another useful feature of an online open scenario repository is a rating system that scores how useful the repository's scenarios are. While users would be able to use searching and/or browsing features to narrow a large set of scenarios down to a small list, it may not be clear which scenarios on the list are most useful for the individual's task. There is great utility in a system that rates the scenarios in the repository.

There are two plausible rating systems that could be used to provide users with feedback about a scenario, a general rating system and a specific rating system. A general rating system would be a simple system that provides each scenario with a number of marks (e.g., "stars") that indicate how valuable the scenario's users, the repository's owners/managers, or both, found the scenario. This general rating system is useful for top-level searches of the repository's content and gives users a general idea of others' opinions of a given scenario.

For more specific searches of the repository's content, a specific rating system would allow previous users of a scenario, the repository's owners and/or managers, or both, to provide guidance to repository users about which scenarios may be particularly useful for a specific activity or set of activities. For example, if a repository user needs a scenario in order to conduct force structure and capability mix analysis, previous users, the repository's owners/managers, or both, could rate how useful a scenario is for force structure and capability mix analysis. This specific rating system would allow repository users to quickly find a scenario that is relevant to their purpose and may improve the quality of the task for which they are using the scenario.

Finally, for both rating systems a set of comments could be provided about the specifics of a scenario by past users and/or the repository's owners/managers. If a previous user found a scenario for their activity, but needed to tailor the scenario more specifically for their needs (e.g., by adding more data) it would be useful for the potential scenario user to know that ahead of time in case they do not have the time or capability to tailor a scenario. Additionally, comments on scenarios would also provide users information about areas in which a scenario may be particularly strong, for example if it has a very detailed timeline. A comments feature would also allow repository users to

evaluate in a timely fashion whether or not they should choose to use a particular scenario.

7. **How do the repository's owners/managers and users communicate and collaborate with each other?**

Similar to a rating system that enables the online open scenario repository's users to provide commentary on individual scenarios, a repository should also have a blog and/or message board that allows both repository users and owners/managers to discuss various issues.

Although similar in purpose, blogs have several distinct differences that make them a more controlled feature than a message board. A blog is run by only a single user or set of users who provide information to others in the form of posts. However, in blogs the opportunities for discussion about original posts are limited since blogs typically allow readers to provide feedback only if it is related to the subject matter of the original post and require the original poster to approve the feedback before it is posted for others to view. The blog format would be useful for an online open scenario repository if the owners/managers wanted a function that would enable them to deliver messages to users in a central location. Conversely, a blog would not be best suited for an online open scenario repository that wishes to provide users with a forum for discussion. In addition, approving any feedback that is posted in response to blog posts could prove to be a cumbersome process for the repository's owners/managers.

If the owners/managers of a repository wished to provide the repository's users an open forum for discussion, a message board would be a preferred feature. A message board is a user driven feature that allows users to post topics that they think are important and encourages other users to post feedback about the topic. If a message board were included in the repository, users would have the opportunity to post topics for discussion by virtue of having access to the repository. Additionally, owners/managers would also post information that is universally important to all of the repository's users. Unlike a blog, however, a message board does not require an approval process for posting, but rather requires a moderator or administrator who polices the board in order to make sure topics are relevant to the repository's purpose.

B. MAJOR VARIABLES AND CONSIDERATIONS

When building an online open scenario repository, other variables and considerations should be carefully considered. One of the variables that need to be

addressed is cost. While it is impossible to provide a cost estimate at this stage of the Open Scenario Study's second phase, it is important to highlight that the cost of a repository will largely be influenced by the relative intensity of the repository's management and support system.[10] If a robust repository with many of the aforementioned features requires labor-intensive management, the initial and recurring costs will likely be larger than a small repository with a management system that requires a lower level of support. Additionally, if the intent is to have the repository grow over time by acquiring many scenarios, it is likely that the demand for more managerial resources will also increase, thereby increasing the recurring cost of the repository.

Another variable that could be used to structure an online open scenario repository is a wiki. The use of a wiki would allow the repository to be a more collaborative website, enabling users to either post scenarios themselves or to make alterations to pre-existing scenarios and posting their changes. A wiki could also enhance the robustness of the repository by exposing users to a breadth of altered scenarios in addition to the original scenarios. However, the inclusion of a wiki in an online open scenario repository would also require the repository managers to regulate user-based postings in order to preserve the quality of the repository's content.

C. ELEMENT ONE AS A STANDALONE APPROACH

In consideration of Element One, an online repository of unclassified scenarios, IDA applied the three selection criteria – Availability, Flexibility, and Responsiveness – to determine whether or not the element could be used as a standalone approach for satisfying the national security community's demand for unclassified scenarios.

Because a repository of unclassified scenarios could be made available on the Internet, and virtually all government agencies and partners have internet access, IDA concluded that Element One could be made available to any and all unclassified scenario users. While the content of the repository may determine who receives access to which scenarios, it could be assumed that anyone demonstrating a substantial need for unclassified scenarios will be granted *some* level of access and only a few, if any, may be excluded. For this reason, Element One more than satisfies the demand of the Availability selection criteria.

---

[10] For example, the Homeland Security Exercise and Evaluation Program (HSEEP) developed for the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) by a contractor is estimated to have cost slightly in excess of $5,000,000.

Also, since the community of unclassified scenario developers and users are frequently faced with changing requirements, there are often changes in existing unclassified scenarios and/or the development of new ones. In order to avoid duplication of effort and maximize cost-efficiencies associated with the modification of existing or development of new unclassified scenarios, it is important that any approach used to meet the demand for unclassified scenarios is responsive to dynamic changes in unclassified scenario content. Therefore, it could also be deduced that given the ease with which any website's content can be changed – especially with the addition of a wiki engine – an online repository of unclassified scenarios would be very responsive to the changing and expanding universe of unclassified scenarios (the Flexibility criteria).

By itself, a repository would not satisfy all aspects of the demand for unclassified scenarios since Element One does offer any solution to users who require a complete or official set of unclassified scenarios or new unclassified scenarios that may not lie in the existing universe. Hence, Element One as a standalone approach, struggles to meet the Responsiveness selection criteria.

Because of the ease with which Element One met the demands of two of the three selection criteria, IDA concluded that an online repository should serve as a foundational element of any approach used to meet the demand for unclassified scenarios. However, it is important to consider Element One's shortcomings with regard to the Flexibility selection criteria. Because of this shortcoming it would be necessary to augment the repository with other elements described in this report. Further elaboration of this point can be found in Chapter VI., which outlines IDA's recommended approach.

D. SUMMARY

Creating an online open repository, Element One, would provide a platform for DoD and its interagency partners to access and use unclassified scenarios. The repository, which receiving received significant support during initial inquisitions in Phase One, would encourage interagency collaboration and cooperation and could become a planning tool, on both operational and strategic levels. In large part, the structure and management system of an online open scenario repository will be dictated by how much of the national security community's demand for unclassified scenarios the project's sponsors wish to meet. While the aforementioned variables are not an exhaustive list, they do help IDA and project sponsors think about the various ways in which a repository and its features should be used to meet the demand for unclassified scenarios.

III. ELEMENT TWO: CERTIFICATION OF EXISTING SCENARIOS

A second potential element of an open scenario approach is a system for certifying scenarios (i.e., Element Two). Certification would provide unclassified scenario users with additional information about a subset of the scenarios that had been judged by an organization or groups of organizations to meet a common set of standards. This chapter outlines the possible purposes of such an element, some variables and considerations for its implementation, and recommends a course of action.

A. DESCRIPTION OF THE ELEMENT

Phase One of the Open Scenario Study defined Element Two as follows: "certification of existing scenarios: designation of [a] pre-existing set of unclassified scenarios as 'preferred' for use throughout [the] community." The first question that this element deals with is what benefits certification would provide. There are two broad potential goals for certification in this context:

- First, certification could simply assist users of unclassified scenarios in sorting or filtering scenarios according to a single set of standards.

- Second, certification could represent an officially expressed preference of the certifying organization for a particular set of unclassified scenarios.

1. Certification as Information for Users

Most likely, any aggregation of unclassified scenarios would contain scenarios with widely varying qualities and characteristics. Simple descriptions of the scenarios might not provide scenario users with all the information they need to filter scenarios that might be appropriate for their use. Especially if there were large numbers of scenario products available, a certification designator for a subset of the scenarios could significantly assist users in conducting this screening process.

The types of standards that might be applied for such a certification will be addressed in the next section, but generally, they would probably focus on descriptive

characteristics of the scenarios that together constitute some measure of quality or completeness. This would allow scenario users to search for scenarios by this criterion.

2. Certification as Organizational Preference

In addition to or instead of the above purpose, certification might serve to indicate preferences of the certifying organization. The notion here is that an organization responsible for evaluating the results of scenario-based analyses, such as the Office of the Secretary of Defense (OSD), the Joint Staff, or the different communities of unclassified scenario users, might use certification as a way of communicating which scenarios in a given scenario library would be most appropriate for use in the decision-making processes to which they are a party. This would imply a different, and probably narrower, set of criteria to be applied for certification, and would also be of interest or concern to a narrower range of potential unclassified scenario users.

These two purposes are sufficiently different that the remaining sections of this chapter treat them separately.

B. MAJOR VARIABLES AND CONSIDERATIONS

Design and implementation of a certification scheme would require addressing several considerations and questions. For each of these, a few different approaches may be feasible, allowing design options to be thought of as "variables." The most important of these variables are:

1. What standards would qualify a scenario for certification?
2. Who would be responsible for certification?
3. In what format would certification be provided?
4. How would operations security (OPSEC) concerns with certification be addressed? (certification as organizational preference only)

In the following section, considerations for each of these questions are addressed in turn.

1. What standards would qualify a scenario for certification?

a. Certification as Information for Users

For purposes of certification as information for users, as outlined above, any number of standards might be appropriate. The most useful standards, however, are likely to be descriptive, as opposed to evaluative. To be useful to the widest possible

audience, the certification might best be geared toward noting the presence of various scenario elements in a scenario, not rating the quality of those elements. The reason for this is the very diverse range of activities in which scenarios are used in the national security community, as demonstrated in Phase One of the study.[11] Ratings of scenario quality would be highly subjective and somewhat variable depending on the intended purpose for the scenario. For example, a scenario with a rich scene-setting premise and little detail on adversary forces might be very well-suited for political-military gaming and very poorly-suited for tactical training.

As a result, the most universally valid set of standards would be a set addressing the extent of the scenario's coverage of different possible features. For example, certification might be given only to those scenarios that address each feature noted within the study's definition of a scenario. In this way, certification becomes a way to indicate a certain threshold level of scenario "completeness" that might be helpful to users filtering the total list of available scenario products.

On the other hand, "completeness" could be considered as just one of several standards applied to a scenario certification process. Other possible criteria include:

- Clarity/organization,

- Plausibility,

- Pedigree of any associated data,

- Validity of threat assessments.

These examples point to the subjectivity any certification judgment beyond completeness would need to be.

b. Certification as Organizational Preference

Certification as organizational preference implies a very different framework for criteria. These would be tailored to the purposes of the certifying organization. Some of the same criteria noted above would be applicable, but greater subjectivity could be justified based on the context of the certifying organization's mission. In this case, certification of unclassified scenarios would become another way for the certifying organization to express its priorities and preferred planning factors to a larger community.

---

[11] *Open Scenario Study, Phase I, Volume 1: Assessment Overview and Results* (IDA Paper P-4326), p. 22.

Standards for this certification would probably touch more directly on the content of scenarios and include considerations such as the following:

- Assumptions regarding U.S. and allied policies, postures, strategies, operations, etc.,

- Country/geographical area addressed,

- Identity and nature of the adversary depicted, and

- The scenario's relationship to other scenarios already created.

2. Who would be responsible for certification?

a. Certification as Information for Users

A few options exist for assigning responsibility for conducting certification as information for users:

- Single organization with scenario expertise (could be from the intelligence community, U.S. Joint Forces Command (JFCOM), Joint Staff, OSD, military departments, etc.).

  - Pros: required knowledge and skill set is available.

  - Cons: no particular incentive for any organization to do it; potential for introduction of organizational bias.

- Representatives from a cross-section of the scenario user community.

  - Pros: enhances credibility of the certification.

  - Cons: labor intensive.

- Scenario contributors certify their own scenarios.

  - Pros: requires least investment of time and resources.

  - Cons: decreases credibility of the certification and/or imposes additional audit requirements.

- Outsource to a qualified Federally Funded Research and Development Center (FFRDC).

  - Pros: FFRDCs remain objective and responsive to government tasking.

  - Cons: trade-off with limited availability of FFRDC resources.

b. Certification as Organizational Preference

Clearly, the options for certification as organization preference are more constrained. By definition, the organization expressing its preferences through the scenarios would need to conduct the certification process. As the central decision-maker on resource allocation and other major programmatic activities, OSD, or an organization designated with certification authority by OSD, is the most likely candidate for such a role. It is currently the most prominent organization in the business of promulgating guidance to other organizations in the form of scenarios. However, since there is a diverse set of needs among those who demand unclassified scenarios, it is possible that individual communities of unclassified scenario users (e.g., the community of users that need unclassified scenarios for force structure and capability mix analysis) could also certify a set(s) of scenarios for their communities use. This option would leverage the expertise of those who know best their community's specific requirements for unclassified scenarios.

3. In what format would certification be provided?

a. Certification as Information for Users

Certification as information for users could take several different forms. The simplest form would be a binary designation of a scenario as either certified or uncertified, based on satisfaction of a single set of criteria. A different type of certification might resemble more of a typology or categorization scheme. This may or may not qualify as "certification," but it would clearly be a useful addition to scenario user searching through a library of unclassified scenarios. A third type of certification would be a rating system that includes multiple levels or tiers. This would necessitate a more subjective approach rating to scenario quality, as opposed to the more descriptive approach.

Whichever form the certification takes, the methodology for applying it would need to be developed and to be generally transparent. Additionally, the certifying body would need to establish a regular schedule for updating certification status of all the scenarios if the recertification of scenarios became necessary.

b. Certification as Organizational Preference

Either the first approach described above (binary rating) or the third approach (multiple levels or tiers) could be applied for certification as organizational preference.

4. How would operations security concerns with certification be addressed? (Certification as organizational preference only)

Apart from more general OPSEC concerns with an open scenario library, there may be security concerns that arise from a particular office being seen to endorse the validity of particular scenarios. DPSs are classified in part due to this concern, and there is no obvious reason why those same issues would not apply to centralized endorsement of an unclassified scenario. One potential work-around for this problem would be to provide certification information offline, via different channels (either classified or unclassified) from the unclassified scenario repository.

C. ELEMENT TWO AS A STANDALONE APPROACH

As a standalone approach, a certified set of scenarios, whether certified as information for users or as organizational preference, would not be easily accessible to the universe of unclassified scenario users unless those responsible for promulgating the certified set take considerable effort to distribute the set *or* those who need them actively sought to attain them for their use. Unlike an online repository, which serves as a shared space for those who need unclassified scenarios and those who develop/distribute them, access to the content of certified sets may be difficult, especially for DoD's external partners, and contingent upon who promulgates and/or certifies the sets and where they are housed in DoD. Given the sporadic distribution of unclassified scenario users throughout DoD and its external partners, IDA concluded that certified sets of unclassified scenarios would be insufficient as a standalone solution given the low probability of a certified set reaching the largest possible number of unclassified scenario users, thus failing to meet the parameters of the Availability selection criteria.

Element Two does not directly address IDA's Flexibility selection criteria. Since the content of unclassified scenarios is often tailored to meet specific user requirements, the sharing of dynamic scenario content throughout the community of unclassified scenario users is important for reducing the duplication of unclassified scenario development efforts and for maximizing cost-savings. While the element does not make either a negative or positive judgment on altering the content of certified sets of unclassified scenarios, it does not directly foster the sharing of dynamic content and, instead, potentially introduces each user to a static set of certified set of unclassified scenarios. If the content of the certified, static sets are altered, the approach does not provide a mechanism for distributing the new content.

However, Element Two is responsive enough to meet different aspects of users' requirements for specific unclassified scenarios. If some communities of unclassified scenarios users wish to have complete or official sets of unclassified scenarios in order to ensure common baselines for studies and analyses, certifying existing unclassified scenarios would help achieve that end by stating, either as an indication of organizational preference or information to users, which scenarios standout among others as part of a complete and/or official set. For these reasons, Element Two does satisfy requirements offered by IDA's third selection criteria (Responsiveness).

In evaluating the applicability of Element Two to an approach aimed at meeting the demand for unclassified scenarios, IDA assessed that the element was not sufficient as a standalone solution. However, as highlighted in previous sections of this chapter, certifying sets of unclassified scenarios does have value and could serve an important role when considered in combination with other elements, especially an online repository of unclassified scenarios.

D. SUMMARY

Based on the preceding discussion, three preliminary insights on the certification element (Element Two) seem apparent. First, certification as user information would be a simpler model to implement, given greater flexibility in selecting some of its key attributes and the absence of questions regarding security and the status of certified unclassified scenarios relative to classified planning scenarios. In the case of certification as user information, the benefit appears tangible, but small. Second, in the case of certification as an indication of organizational preference, the desire to have a new, complete, or official set of unclassified scenarios can be satisfied by having an organization designate an existing amalgamation of scenarios as such. With some organizations requiring such sets, the benefits appear both important and potentially impactful on the way organizations use and perceive the value of unclassified scenarios. Third, Element Two could not sufficiently serve as a standalone component of an approach towards meeting the demand for unclassified scenarios and would be better suited if paired with Element One, an online repository of unclassified scenarios.

IV. ELEMENT THREE: DEVELOPMENT OF A NEW UNCLASSIFIED SCENARIO SET

Whether for the establishment of a common unclassified scenario development process or generating a small number of scenarios to fill gaps in a preexisting set(s) of scenarios, understanding how DoD might develop unclassified scenarios is important to the construction of an approach designed to meet the demand for unclassified scenarios (Element Three). This section addresses Element Three and explores various options for developing new unclassified scenarios as a coordinated official set or simply as "gap-fillers" for already existing unclassified scenarios from various sources.

A. DESCRIPTION OF THE ELEMENT

Current classified defense scenario development activities are critical throughout DoD and are an important component of an increasingly diverse and dynamic U.S. national security community. Within the Office of the Under Secretary of Defense for Policy (OUSD(P)), the classified Defense Planning Scenarios (DPS) are developed through a codified, institutionalized process within DoD's Analytic Agenda framework.[12] DoD maintains a centralized capacity for developing an official set of classified DPSs that are used throughout the Department and developed in a consistent and integrated fashion. Classified DPSs also possess an official standing throughout DoD, and OSD directs the use of DPSs in various DoD-wide defense planning activities such as Planning, Programming, Budgeting, and Execution System (PPBES) deliberations and the Quadrennial Defense Review (QDR).

OUSD(P)'s existing DPS enterprise (e.g. organization, personnel and practices) produces a set of classified scenarios within an established, institutionalized and centralized framework that is mature and supported by comprehensive methodologies and consistent processes. OUSD(P)'s DPS enterprise and its scenario products are a widely utilized resource and recognized authority. This chapter examines the possibility of

---

[12] For general background on the Analytic Agenda and the development of DPSs see Appendix B of this report.

developing new unclassified scenarios by leveraging, in some capacity, the existing DPS framework or outsourcing unclassified scenario development to organizations outside DoD.

Outlined below are examples of four organizational concepts for producing new unclassified (DPS-like) scenarios. Each organizational concept aims to support the growing demand for unclassified scenarios within DoD and among external partners. In addition, each organizational concept lends support to addressing broader challenges associated with the development of ad hoc scenarios, such as the lack of standardization, coordination and collaboration.

While each of the four concepts is unique, all are aimed at leveraging OUSD(P)'s current institutional capacities used to produce classified DPSs. The four concepts are:

1. expand the capacity of OUSD(P)'s existing DPS enterprise;

2. replicate a parallel but independent and unclassified DPS enterprise;

3. evolve an OUSD(P) centrally led but distributed implementation model; and,

4. privatize unclassified DPSs outside of DoD.

Highlighted next is a general description and initial discussion of each of these organizational concepts that might be used to produce new DPS-like, unclassified scenarios.

1. Expand OUSD(P)'s Existing Defense Planning Scenario Enterprise

This concept includes leveraging the current institutional capabilities and infrastructure resident within the existing DPS enterprise and expanding its capacity to produce official unclassified scenarios. As mentioned, OUSD(P)'s existing DPS enterprise is in a unique position as the exclusive purveyor, producer, and distributor of DoD's only official set of classified scenarios. OUSD(P)'s DPS enterprise is the recognized authority of related activities and DPSs are widely utilized throughout DoD.

Of equal importance are the broader benefits of incremental expansion of DPS's existing capabilities and current offerings to include unclassified scenarios in support of promoting increased commonality in scenario development and implementation (e.g., standardization and coordination). These collective needs are increasingly important to meet the growing demand for greater collaboration and integration of DoD's internal and external scenario-related activities, particularly as they relate to DoD's current ad hoc scenario efforts. This concept also presents the greatest opportunity to potentially

minimize the cost, risk, and time inherent in a new start-up venture, because this option leverages OUSD(P)'s established DPS scenario development processes and organizational infrastructure.

2. **Create a Parallel (but independent) Defense Planning Scenario Enterprise for Unclassified Scenarios**

This second concept involves replicating OUSD(P)'s existing DPS enterprise model and reconstituting it within a newly formed and independent organization. This organization with OSD-level authority would adopt established know-how and expertise of the current DPS enterprise; although this new entity would remain independent as a protective measure against potential comingling of classified material and related activities. This concept might also reduce the complexity of integrating and concurrently managing classified and unclassified processes needed to support two different OPSEC systems within a single DPS organization. In addition, given this concept's cloning feature of an established DPS enterprise model, this concept might also limit start-up risk and setup time compared with demands typical of creating and launching an entirely new organization.

However, creating a second parallel organization for the sake of segregating two similar organizations for security reasons could be an inefficient use of substantial resources. This concept might also result in additional organizational barriers and increased bureaucratic impediments to the growing need for greater coordination, collaboration and integration of scenario-related activities (both unclassified and classified) within DoD and among its external partners.

3. **Evolve OUSD(P)'s Existing Defense Planning Scenario Enterprise into a Distributed Organization**

This concept incorporates benefits presented in the first concept (i.e., utilizing the existing DPS enterprise, capabilities, know-how and official standing) while also leveraging the value of DoD's ad hoc and decentralized unclassified scenario efforts. The unique difference of this third concept is the notion of a central DPS enterprise establishing a distributed network of certified DoD scenario developers operating independently and outside of, but in collaboration with, OUSD(P)'s existing DPS framework. As stated earlier, numerous decentralized and ad hoc scenario development activities exist within DoD. It is likely that many of these disparate organizations possess specialized and significant scenario-related capabilities (e.g., expert knowledge of common functional capabilities, unique expertise in key technology areas, and

particularly close linkages to critical warfighter capabilities). Given that many such organizations are already actively involved in related scenario development activities of DoD-wide importance (both classified and unclassified), it would be beneficial to support greater integration of ad hoc scenario efforts throughout DoD.

Leadership of OUSD(P)'s centralized DPS enterprise would decide on which of its individual unclassified scenario requirements ought to remain in-house (i.e. within OUSD(P)) and which should to be outsourced to a distributed network of certified but independent scenario developers. While some level of ad hoc scenario development activities will likely inevitably continue throughout DoD, constructively reaching out to and engaging subordinate organizations would promote opportunities for greater coordination and collaboration among DoD's ad hoc and disparate scenario developers. Resulting behaviors and interactions would further encourage greater DoD-wide uniformity and efficiencies in scenario building (e.g. standardization, sharing of common practices and greater optimization of existing expertise and resources).

4. Outsource Unclassified Scenario Functions to the Private Sector

This concept proposes incorporating relevant aspects of concepts one through three above with the notable exception of outsourcing the bulk of DoD's future capabilities in unclassified scenarios to the private sector.

However, unlike the second concept, the day-to-day implementation would not be carried out at the level of autonomy envisioned for a parallel government DPS enterprise. To the contrary, DoD would maintain ownership and control of a future unclassified scenario development enterprise, albeit at an appropriately high level. Related OUSD(P) roles would include those uniquely governmental in nature and consistent with existing contractor relationship standards -- such as providing contractor direction, operating requirements, performance metrics and insuring accountability.

Given the globally dynamic and fast changing environment of scenario development practices, a growing need to expand beyond DoD, coupled with the value of maintaining existing OUSD(P) core competencies possessed within the current DPS framework -- it might be particularly beneficial to encourage creative teaming relationships between diverse sectors of service providers. For example, teaming an experienced FFRDC with a university-based scenario leader and a leading-edge scenario consultancy could yield products capable of addressing the challenges presented by quickly evolving civil-military operational environments.

B. MAJOR VARIABLES AND CONSIDERATIONS

Unclassified scenario development activities of a single DoD subordinate organization, such as the Army's MLS development process, often become stove-piped and unable to contribute to solutions dependent on multi-Service (Joint) capabilities. Of additional concern is the adverse effect of DoD's ad hoc scenario activities that may impact collaboration with U.S. interagency efforts and partnerships with state-local government as well as DoD interactions with foreign allies and international non-governmental organizations (NGOs). Many such scenario development activities and implementation efforts warrant an OSD-level, DoD-wide approach to developing official unclassified scenarios. Additionally, the growing tendency towards multinational and civil-military operations runs counter to singular approaches to scenario development.

This is not to say there is no value or role for DoD subordinate organizations in unclassified scenario development. Numerous circumstances likely exist whereas the best approach to a particular unclassified scenario is more effectively satisfied at the level of an individual Defense Component organization (e.g., Combatant Command (COCOM), Military Services, or Defense Agencies). For example, the U.S. Army developed the MLS which provides an example of an existing codified institutionalized process that could be utilized while developing an approach for meeting unclassified scenario demand. The MLS provides a similar structure to the DPS-derived scenarios but avoids issues of classification and life span. As noted by IDA earlier in this report, the MLS's disadvantage is that it is Army-centric and other Services are not actively participating in the development process.[13] While such efforts should be visible and shared throughout DoD, and should make use of common scenario standards and processes to the extent practical, it would be impractical and counterproductive for OSD to assume responsibility for unclassified scenario development activities under all circumstances.

Conversely, it would be similarly inappropriate for DoD subordinate organizations to undertake the development of unclassified scenarios encompassing DoD-wide domains and or broad scale external partnerships (e.g., U.S. interagency and foreign allies) without direction and coordination of DoD. For many such circumstances, a DPS-like approach to developing unclassified scenarios by an organization with OSD-level authority would be optimal.

---

[13] For more information on the Army's MLS, see Appendix E of this report and *Open Scenario Study: U.S. Army's Multi-Level Scenarios Sub-Task* (IDA Paper-P 4466).

While DoD and its components have important roles to play in developing a future set of unclassified scenarios, OSD needs to play a central role in any process similar to OUSD(P)'s production of DPS-like, unclassified scenarios while also delegating or outsourcing the production of certain unclassified scenarios to OSD subordinate organizations as warranted.

A key aspect of OSD and subordinate organizations participating in the development of new unclassified scenarios is the importance for both parties to utilize common standards, uniform processes and shared best practices. Without such commonality, coordination and cooperation, future DoD integration of related efforts will likely be impeded.

Also noteworthy and of value to DoD is the existence of unclassified scenario development activities and products occurring outside of DoD. External development and use of open scenarios is expansive and supported by a variety of U.S. and foreign organizations including state and federal governments as well as civilian law enforcement and allied militaries. Scenario activities are also prevalent among diverse and increasingly globalized industries, think tanks, academic institutions and NGOs. However, efforts are typically uncoordinated as well as difficult to track, while associated scenario development and implementation activities might often lack standardization, integration and sharing of common best practices. Nonetheless, these non-DoD scenario development activities and their scenario products may be of considerable value to DoD as it seeks to develop new unclassified scenarios. Therefore, the inclusion of civilian agencies in the scope of the Open Scenario Study, and the examination of Element Three, is important to ensure a holistic and well-rounded approach to satisfying DoD's demand for unclassified scenarios.

A key aspect of whether or not OSD (or a designated subordinate organization) generates a new unclassified scenario is largely determined by whether or not a relevant unclassified scenario already exists within DoD or elsewhere. As discussed in Chapter III. of this report, one option that could be used to satisfy the demand of unclassified scenarios would be to certify preexisting unclassified scenarios. As such, a process is needed to help determine if a specific scenario gap exists within an open scenario repository which would lead DoD to produce a new unclassified scenario in order to satisfy future scenario requirements.

This also implies a significant difference between a future set of DPS-like, unclassified scenarios and the current set of classified DPSs. Namely, certified (and

likely modified) ad hoc DoD unclassified scenarios from sources throughout the Department, along with similarly qualified non-DoD unclassified scenarios, would populate portions of a future set of unclassified scenarios.[14] However, scenario gaps would likely exist within the open scenario repository that would consequently result in gaps within an unclassified scenario set that would subsequently be filled by the creation new unclassified scenarios.

C. ELEMENT THREE AS A STANDALONE APPROACH

When evaluated by the three selection criteria – Accessibility, Flexibility, and Responsiveness – Element Three does not suffice as a standalone approach for meeting the existing demand for unclassified scenarios. Three of the four concepts discussed in this chapter develop new unclassified scenarios by leveraging the existing DPS enterprise in some capacity. Using any of these three variations of Element Three as a standalone approach would make any newly developed scenarios available to a large audience of scenario users considering that classified DPSs are readily available throughout DoD. Since many of DoD's external partners are a large part of the wider community of unclassified scenario users, it is unlikely that they would have easy access to any new scenarios developed using a variation of the DPS framework unless a cognizant effort is made to include them. This problem is difficult to ignore given that one of the primary reasons unclassified scenarios are used is *because of* the need to collaborate with external partners. The fourth concept, outsourcing unclassified scenario functions to the private sector, may face similar obstacles since the development process is moved entirely outside the Department. While Element Three as a standalone solution would be available to a wide cross-section of unclassified scenario users, it is not the optimal approach.

As a standalone approach, Element Three would have difficulties making changes in scenario content available to the community of unclassified scenario users (Flexibility selection criteria). While any of the four concepts discussed in Element Three would, undoubtedly, make *new* unclassified scenarios available to *some* unclassified scenario users, Element Three itself is not inherently conducive to sharing user-driven scenario content and alterations as it makes no effort to distribute such content. Because of this, user-made changes to the existing body of unclassified scenario content would not be

---

14   See Chapter III, Element Two: Certification of Existing Scenarios, of this report for related details on certification of existing scenarios developed by DoD and non-DoD organizations.

shared throughout the community and duplication of scenario development efforts would still exist throughout the community.

Any of the aforementioned descriptions of Element Three would be relatively responsive to the varying aspects of users' demand for unclassified scenarios. If users of unclassified scenarios require complete, official, or new sets of unclassified scenarios for their activities, any of the four concepts discussed in the preceding sections of this chapter would suffice as each concept could potentially offer all three. Therefore, Element Three does have some utility to contribute to an approach designed to meet the national security community's demand for unclassified scenarios.

Because Element Three would not be available to the largest possible audience of unclassified scenarios users and does not inherently foster the sharing of changes in existing unclassified scenario content, it is inadequate as a standalone approach to meeting the national security community's demand for unclassified scenarios and should instead be considered in combination with other elements reviewed in this report.

D. SUMMARY

There are multiple organizational concepts that can be used by DoD to produce new unclassified scenarios (Element Three). The four concepts include:

- Expand OUSD(P)'s existing DPS enterprise.

- Create a parallel (but independent) DPS enterprise for unclassified scenarios.

- Evolve OUSD(P)'s existing DPS enterprise into a distributed DPS enterprise.

- Outsource unclassified scenario functions to the private sector.

Any of these four DPS-like organizational concepts could support a broader construct for creating a "one-stop-shop" capability that integrates other components of the major elements discussed in this report. However, using Element Three as a standalone approach for satisfying unclassified scenario demand would not be ideal. "Bundling" elements introduced in this report would potentially afford increased efficiencies and productivity improvements as well as promote greater commonality, collaboration and integration of related scenario development and implementation practices.

V.   ELEMENT FOUR: DECLASSIFICATION OF CLASSIFIED SCENARIOS

This chapter discusses the element of declassifying scenarios, to produce official unclassified scenarios (i.e., Element Three), by identifying and removing sensitive material in classified DPSs. The goal of developing a means to declassify DPSs is to create a cost-effective process that is not more costly than current methods for developing unclassified scenarios and can create an unclassified set of scenarios equivalent to the DPSs. However, as will be explained later in this chapter, there are several reason why the declassification of classified scenarios should *not* be considered a key element of an approach to better meet the demand for unclassified scenarios.

A. DESCRIPTION OF THE ELEMENT

Currently there is not an approved process for declassifying existing scenarios or vignettes used in DoD's Analytic Agenda.[15]   Possible actions that could be taken to declassify DPSs include:

1. varying the level of detail in DPSs according to the priority or nature of the analysis or exercise to be conducted so the scenario could be unclassified and approved for public release, or

2. generalize existing scenarios with fictional locations and forces.

These actions would create scenarios with different levels of details depending on priority or nature of the operational challenge depicted such as strategy, road to war, force lists, and other data. The Joint Data Support (JDS) office, of Office of the Secretary of Defense for Cost Assessment and Program Evaluation (OSD (CAPE)), provides support for the identification, collection, development (including verification and validation), management, and dissemination of data and associated analytical baselines for the Analytic Agenda process. An unclassified version of the JDS support process could be employed to provide the same level of service for an unclassified DPS

---

[15] See Appendix B of this report for more information on DoD's Analytic Agenda.

process. OSD (CAPE) would be the logical organization to perform this function. CAPE collects data needed to populate its databases from the Services and intelligence agencies. Potentially, CAPE could populate an unclassified version of the JDS website using open sources instead of input from the Services and intelligence agencies or ask for unclassified data such as generic tables of organizations and equipment for military units. Finally, there are outside sources of unclassified data such, as *Jane's* publications[16] that could be used to supplement the unclassified versions of scenarios and vignettes. Using these sources of unclassified data should simplify the sanitization process and fill in gaps left by the removal of classified information.

B. MAJOR VARIABLES AND CONSIDERATIONS

The first challenge to declassifying DPSs and vignettes would be to determine which ones could be declassified and have applicability to requirements to conduct exercises with interagency, foreign militaries, and state and local governments. After determining which scenarios should be declassified, it would be necessary to decide which classified data must be replaced with open source data to keep the scenario viable for use for an unclassified purpose. This would be a difficult and time consuming task if the development of the unclassified scenario or vignette is sequential to the development of the classified version because each classified data source will have to be re-visited to be verified and a determination made as to what makes the data classified. A decision regarding how to best replace the data would also need to be made, and the actual location and placement of the substitute data would follow.

Additionally, many DPSs and vignettes gain their value through the depiction of classified operating environments and U.S. capabilities. These scenarios and vignettes may be difficult, if not impossible, to sanitize. It is entirely possible that by sanitizing such scenarios or vignettes they lose their value all together and would be of no more utility than unclassified scenarios developed outside the Analytic Agenda process.

Even though some DPSs can be sanitized and would have unclassified applications, there are some organizations that would argue that an adversaries' ability to aggregate unclassified data would still present a classified picture of U.S. military capabilities. An example of this "aggregate knowledge" argument is the substitution of specific military units with generic units or the substitution of an actual country with a

---

[16] HIS Jane's Information Group, available at www.janes.com. Accessed on January 28, 2010.

fictitious country name. One might argue that U.S. adversaries have sufficient knowledge of U.S. military units and could therefore deduce which units would respond in a particular scenario or that the main features and characteristics of the fictitious country match too closely with the actual country. It is hard to argue against this logic because it is impossible to prove that U.S. enemies would not arrive at the same decisions as U.S. decision-makers.

The pros are that *some* DPSs can be sanitized and still act as a useful scenario. This option leverages an existing process and scenarios, thereby reducing the necessity of having organizations develop new unclassified scenarios. A major con is that some organizations in the Analytic Agenda process may object to the sanitized version based on the "aggregating unclassified data" of U.S. military capabilities argument. Additionally, many classified scenarios will also lose their value as unclassified products since classified information may be largely responsible for their utility. Accordingly, retroactively sanitizing existing DPSs would not be an effective use of resources or may not add any value that is not already gained through status quo unclassified scenario development processes.

C. ELEMENT FOUR AS A STANDALONE APPROACH

In consideration of Element Four, the declassification of classified scenarios, IDA applied three selected criteria (Availability, Flexibility, and Responsiveness) to determine whether or not the element could be used as a standalone approach for satisfying the national security community's demand for unclassified scenarios.

As a standalone approach, the declassification of classified scenarios fails to meet the requirements set forth by IDA's Availability selection criteria. The process of declassifying classified scenarios, by itself, does not offer a mechanism that makes the newly declassified scenarios available to those who would use them. Unless the process is coupled with a distribution platform, for example an online repository, the declassified scenarios would not be distributed to a wide enough audience to warrant their deployment as a standalone option.

The process of declassifying currently classified scenarios, when used as a standalone approach to satisfy unclassified scenario demand, does not meet the parameters of the Flexibility selection criteria. The criteria require that a deployed approach be flexible enough to make changes in unclassified scenario content available to the rest of the unclassified scenario user community. While the declassification of classified scenarios does offer a new set of scenarios to users, by virtue of releasing a

substantially altered set of scenarios, the element does not facilitate or enable the distribution of user-adjusted unclassified scenario content. Therefore, Element Four, when used by itself, cannot fully account for the user-driven dynamic of unclassified scenario demand.

The declassification of classified scenarios may be somewhat responsive to varying aspects of users 'demand for unclassified scenarios,' but would likely need to be coupled with another element, such as Element Two, certification as an indication of organizational preference, for its potential to be maximized. It can be imagined that if *all* of the DPSs were declassified, they could be offered to the community of unclassified scenario users as an official, complete, and/or new set of unclassified scenario users. However, it is also possible, and in fact likely, that when stripped of their classified information and data the scenarios lose their official standing since it is the depiction of that sensitive information and data which give the scenarios their authority as an official and complete set in the first place. In all likelihood, because the scenarios have lost some of their value during the declassification process, and consequently, their official standing, they would need to be recertified by a parent organization in order to regain their authority *if* the organization thought the newly declassified scenarios were of sufficient quality.

In evaluating the applicability of Element Four in meeting the demand for unclassified scenarios, IDA assessed that not only is the element not sufficient as a standalone solution, but it need not be a component of the recommended approach designed to meet the existing demand for unclassified scenarios.

D. SUMMARY

Declassifying DPSs and vignettes is feasible and may help build a validated set of unclassified scenarios that mirror the DPSs. The greatest unknown variable of Element Four is how difficult it will be to get agreement on what constitutes a sanitized DPS and identify useable open sources to populate the gaps left by the removal of classified information and data. Additionally, many DPSs and vignettes would lose their utility after the declassification process since their greatest asset is the discussion of classified challenges, operational environments, concept of operations (CONOPS), and forces and capabilities data. These challenges, coupled with the fact that it is not a preferred element of an approach by IDA's government sponsors, lead to the assessment that Element Four need not be a component of an approach designed to meet the existing demand for unclassified scenarios.

VI. RECOMMENDED APPROACH

The purpose of this chapter is to provide IDA's recommended approach for better satisfying the demand for unclassified scenarios. The chapter also provides guidance for how the approach should be constructed and the elements that should be used in its design.

A. POTENTIAL APPROACHES

After a detailed exploration of each of the four individual elements, IDA determined that Element Four, declassifying classified DPSs, would be a costly and time consuming process and would a require a process where it is difficult to gauge whether or not a given DPS has been sufficiently sanitized. It was also determined that many DPSs would lose their utility after the declassification process since their greatest asset is often the discussion of classified challenges, operational environments, CONOPS, and forces and capabilities data. Thus IDA concluded that Element Four should not be a component of an approach aimed at satisfying the national security community's demand for unclassified scenarios.

Additionally, IDA examined the possibility of each of the other elements serving as a standalone approach for meeting existing demand for unclassified scenarios. However, as the previous chapters indicate, none of the elements performed well enough against the selection criteria to serve as a standalone component of an approach.

Finally, IDA also took into consideration that during Phase One and through iterative interactions with the project's government sponsors, unclassified scenarios developers, and users in Phase Two, that there is a strong preference for an online open repository of unclassified scenarios. Subsequently, IDA's sponsors approved the launch of a proof-of-principle online open scenario repository beta site at the start of Phase Two. This beta site could serve as a foundation for a more complete approach, since it can easily be modified into a more robust, highly capable platform.

Logically, with the preference for Element One and exclusion of Element Four, four potential approaches exist:

1. **Open Scenario Repository** – House or link existing unclassified scenarios, developed by any available sources, in a searchable, online virtual space (Element One).

2. **Certify and House Existing Unclassified Scenarios in a Repository** – Certify existing unclassified scenarios to create an official set of unclassified scenarios that is housed in an online repository (Element One and Element Two).

3. **Housing Newly Developed Scenarios in a Repository** – Develop a new, official set of unclassified scenarios and house them in an online repository (Element One and Element Three).

4. **Certify Existing and Develop New Unclassified Scenarios and House in a Repository** – Certify existing unclassified scenarios and develop new unclassified scenarios to create an official set of unclassified scenarios that is housed in an online repository (Element One, Element Two, and Element Three).

When constructing an approach designed to meet the demand for unclassified scenarios, it is necessary to use the previously described elements in combination, rather than individually. Previous chapters of this report demonstrated that using any single element alone as an approach will not make the approach available to the largest possible audience of unclassified scenarios users, cannot easily share and distribute changes to unclassified scenario content to users, and are not adequately responsive to the varying aspects of unclassified scenario users' demand for unclassified scenarios.

One approach from the aforementioned list, Approach #4, was selected to explore in-depth, for several reasons. First, Approach #4 more than adequately meets the three criteria (Availability, Flexibility, and Responsiveness) that each of the individual elements has been measured against. Because Approach #4 includes an online repository, accessible via the internet, it would be available to the largest possible audience of unclassified scenario user, which satisfies the requirements of the Availability criteria. Also, since the approach would enable, through its management system and key features such as a wiki engine, the inclusion of the current and future universe of unclassified scenarios the approach would make changes in unclassified scenario content readily available to the community of unclassified scenario users, satisfying the requirements of the Flexibility criteria. Finally, because the approach calls for the certification, as an indication of organizational preference, of existing scenarios *and* the development of new

unclassified scenarios, the approach would be responsive to users that require complete, official, and/or new sets of unclassified scenarios, which satisfies the requirements of the Responsiveness criteria.

B. IDA'S RECOMMENDED APPROACH

IDA recommends that DoD certify selected existing unclassified scenarios (for example the Army's MLS 1.0 and 2.0) (Element Two) based on the preferences of the individual unclassified scenario user communities identified in Phase One, and develop new unclassified scenarios as needed through a distributed development model (Element Three) to create an official set(s) of unclassified scenarios. These scenarios and other existing unclassified scenarios should be housed in an online repository (Element One).

IDA's recommended approach seeks to create a multiple "complete" set of unclassified scenarios and house them in an online repository. In order to create complete sets of unclassified scenarios, the recommended approach leverages existing unclassified scenarios by certifying some of them, at the discretion of individual unclassified scenario user communities' preference, and including them as part of a preferred set, should they meet that community's pre-designated set of certification criteria. However, building a "complete" set of unclassified scenarios is a highly subjective activity. Each individual community of unclassified scenario users would assign a decision-making body the task of deciding what constitutes a "complete" set of unclassified scenarios. For example, it may be decided that a complete set of unclassified scenarios is an aggregation of scenarios that cover certain geographic regions of the world or are conducive to studies and analyses for a given taxonomy of functions.[17]

If existing unclassified scenarios do not meet all of the standards set forth by any given community's decision-making body responsible for promulgating a complete set of unclassified scenarios and there are gaps in the set, then the recommended approach requires the development of new unclassified scenarios in order to successfully build a complete set of unclassified scenarios. The process of developing new unclassified scenarios would be similar to the process described in the "Evolve OUSD (P)'s Existing DPS Enterprise into a Distributed Organization" section of Chapter IV., which describes and analyzes Element Three. However, the main contrast between IDA's recommended

---

[17] For example, force structure and capability mix analysis, acquisition, concept development and experimentation, wargaming, training and education, testing, intelligence and threat assessment, and operational planning.

approach and the option presented in Chapter IV. is that the development of the new scenarios would not necessarily have to mirror-image OUSD (P)'s DPS process, but could use any variation of the process instead. After the development of the new scenarios, the complete set would be housed in the online repository. The process of creating/building the recommended approach is illustrated in Figure 2.
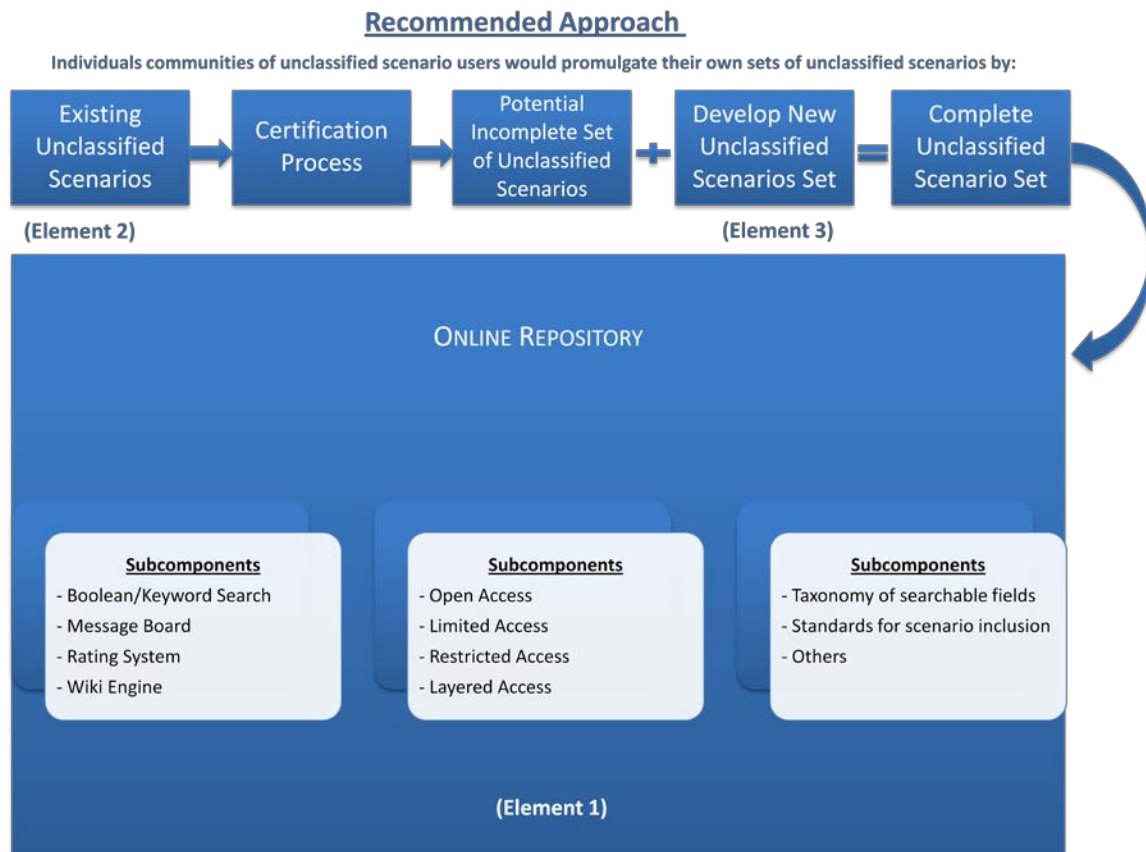
Figure 2. Recommended Approach

This figure graphically depicts each of the elements and steps that may be needed to construct the recommended approach. First, individual communities of unclassified scenario users will attempt to make an official set of unclassified scenarios by certifying existing unclassified scenarios as such. If the aggregation of existing unclassified scenarios yields a set of scenarios that is insufficient in quantity or quality, new unclassified scenarios would be developed to complete the official set, which will then be housed in the online repository.

C. THE REPOSITORY

1. Repository Features

The recommended repository would include features such as a search engine, a Wiki engine, feedback form, blog and message board.

a. Search Engine

Perhaps the most important functional feature of the repository will be its search engine. The best way to fulfill this requirement is to design the repository as a summary database with a basic query capability that enables Boolean and keyword searching. Because the repository will provide users with a variety of information on each scenario, library searching, based on taxonomy of database fields, should be a simple task.[18] With a Boolean search feature users will have the option of typing queries using logical operators such as "AND", "OR", and "NOT". For example, if a repository user wants to find the listings of unclassified scenarios dealing with a particular geographical region (Africa) and specific military operations (Major Combat Operations) s/he can use the simple search equation "Africa" AND "Major Combat Operations" to receive the most relevant listings.

In addition, the repository should also be equipped with an advanced search function that allows users to conduct searches within specific fields, rather than the across the entire repository. Such a function would also allow users to enter search terms across multiple fields: for example, by inserting the term "Africa" in the Geographic Region field; the term "Major Combat Operations" in the Military Operations Depicted field; and the term "2025" in the Timeframe field.[19] The advanced search function would also mimic options that are found in most user-friendly search engines, such as Google, by allowing users to find scenarios using such standard searching operations as "exact phrases" and "all these words."[20]

Recommended Action: The repository should be a summary database with basic query capability that enables keyword and Boolean search queries. The repository should also

---

[18] See Appendix C of this report for the current list of fields in the taxonomy. This taxonomy is amendable and not thought to be final.

[19] A drop down menu for each field is also an option.

[20] See, for example, *Google Advanced Search* at http://www.google.com/advanced_search?hl=en: accessed January 28, 2010.

be equipped with an "advanced search" function that allows users to type in more than one specific search term and to search within specific fields, rather than across the entire repository. An online unclassified scenario repository may need to house many hundreds, if not thousands, of scenarios that differ in the number of components used to build the scenario and their level of detail. As a separate function, it would also be useful to display the repository's scenarios in list format as well, so that users may browse the repository.

b. Wiki Engine

Another feature that could be used in an online open scenario repository is a wiki engine. Using a wiki engine would allow for a variety of other functions such as a user-based rating system, feedback submission, and the posting of new or altered scenarios. If each scenario were presented on a unique, wiki-based page, which then linked directly to the scenario, users would have the opportunity to post their feedback regarding the scenario's utility for a given function (*e.g.*, "Scenario X is particularly useful for multilateral training and exercise events") or on any other issues. These comments could then be reviewed by other repository users and may influence their decision whether or not to use a scenario for a particular activity.
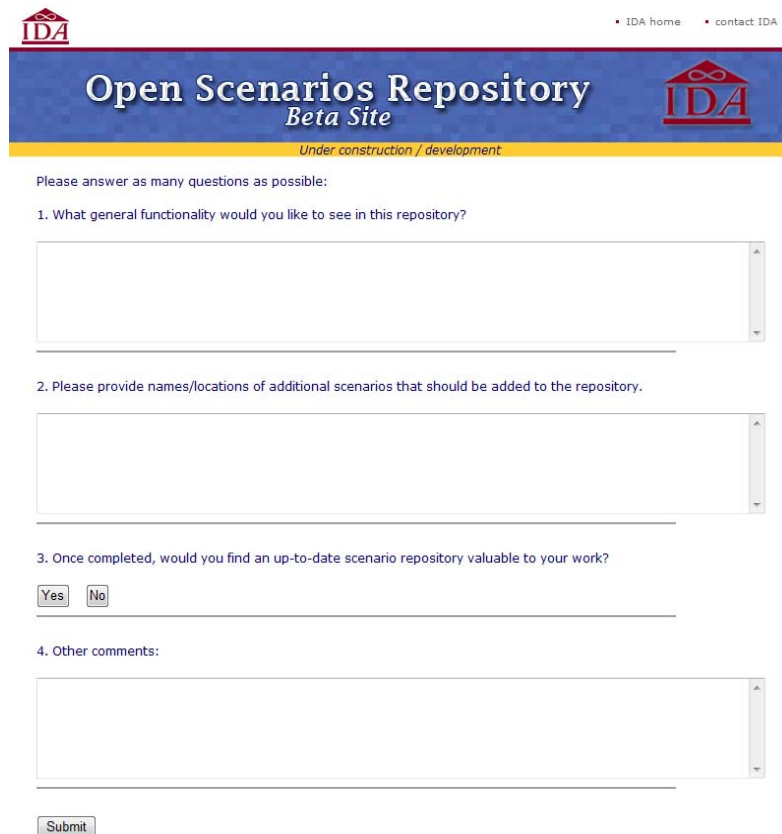
In addition to being conducive to allowing user feedback, a wiki engine would also allow the repository to essentially populate itself. Users could post new scenarios to the repository by attaching the scenario to a wiki page and filling in each of the fields with relevant information. Additionally, users may also re-post scenarios after they have been tailored and used for any number of activities.

While the wiki engine would make populating the repository less labor-intensive, the use of a wiki would not exempt the repository owner(s) from making some decisions regarding the site's content. In order to preserve the integrity and usefulness of the repository, it would be best if new or edited scenarios were reviewed by the repository owners before being posted to the site. This could easily be done by ensuring that the repository owner(s) receive an automated e-mail requesting their approval of new and altered scenarios before they are posted to the repository. After receiving an automated e-mail notifying them of a request for additions to the repository's content, the owner(s) would examine the new or edited scenario(s) and decide whether or not they should be included in the repository. For a complete discussion on standards for including a new or edited scenario in the repository, see 2.b."Standards for Including a Scenario in the Repository: A Tiered Approach," later in section C. of this chapter.

Recommended Action: Equip the repository with a wiki engine. Enable the wiki engine to allow users to post new or edited scenarios to the repository, provide feedback on scenarios, and rate scenarios according to their utility for a given application.

c. Feedback Form, Blog and Message Boards

If a repository is to meet the repository users' demand for unclassified scenarios effectively, it is imperative to include features that allow easy communication between the repository's users and manager. One such feature is a feedback form, which would allow users to provide the repository managers with meaningful commentary regarding the content and functionality of the repository. One example of such a form already exists at (see Figure 3).

Figure 3. Sample Feedback Form

The feedback form depicted above is an example from IDA's online Open Scenario Repository Beta Site, which is located on the website

http://openscenarios.ida.org/pages/feedback.html.

The form asks users what general functionality they would like to see in the repository, the names/locations of additional scenarios that should be included in the repository, and provides a space for other comments.[21] Users may fill out these questions and submit them to the repository managers at any time. In order to ensure that repository users feel comfortable providing honest feedback, the feedback form could also provide an option for anonymous submittals.

Another feature that would allow communication between the repository's users and managers is a manager-run blog. A blog could serve as a front page to the repository, allowing the managers to update users regularly with "news" regarding additions, subtractions, and/or changes to the repository's content, functionality, and management features. This feature should also have a comments section underneath that allows users to ask the repository managers questions about any individual update and allow the managers to respond directly to those questions.

In addition to a feedback form and blog, an online open scenario repository should also have a message board. A message board would allow communications between repository users by enabling them to start threads on any given scenario-related topic. Threads would be separated into larger categories for easy browsing and would allow users to view messages on topics of interest. Under the message-board schema, there would be a specific board for any given user community – force structure and capability mix analysis, for example. If a user has an interest in or is part of the force structure and capability mix analysis community, then s/he could browse or start threads under this message board category, as well as post to any existing thread. Among things that users might post are: discussion on the best way to use/modify scenarios in the repository, how to conduct certain analyses with scenarios, questions regarding the specifics of a scenarios, requests for recommendations on how best to use a specific scenario, or even information about relevant, upcoming scenario-related events. Because of the high volume of traffic the repository message board might receive, it would also be useful and convenient for the repository's managers to also post relevant information there.

Recommended Action: A repository should include a blog that allows the repository's managers to post news and updates, a feedback form that allows repository users to comment directly and anonymously, if desired, to the repository managers regarding the

---

21 This is a notional list of questions. The feedback form in a more robust repository should have a more comprehensive set of questions.

site's functionality and content, and a message board that enables discussion on a variety of topics between repository users.

2. Repository Access and Scenario Inclusion

The following items should be considered when developing the repository: levels of access, how to include scenarios, and where the repository should be stored.

a. Levels of Access

It would be optimal for the repository to be accessible to anyone who needs to use unclassified scenarios for their tasks. However, due to OPSEC concerns, it may not be in the best interest of the repository's government owner(s) to allow complete, open access to the entire library of unclassified scenarios cataloged in the repository. A repository with completely open access would not only allow potential adversaries to gain an understanding of how the U.S. government conducts its planning efforts using scenarios, but would also subject the repository's owner(s), and DoD or the U.S. federal government as a whole, to unwarranted publicity regarding sensitive issues that any scenarios housed in the repository may contain. Phase One of the Open Scenario Study discovered that one of the highest sensitivities surrounding *some* unclassified scenarios is the fact that they are affiliated with the U.S. federal government and/or DoD. Unclassified scenarios can be perceived, rightly or wrongly, to be government assessments regarding the plausibility or possibility of future challenges and/or threats depicted in the scenario. Additionally, there is also the potential for the perception that unclassified scenarios depicting interactions with certain states may also represent official U.S. policy towards them. Therefore, in order to avoid misperception, it may not be advantageous to make some unclassified scenarios available in the public domain. Additionally, a repository with completely open access would not allow for the inclusion of For Official Use Only (FOUO) scenarios, Sensitive But Unclassified scenarios (SBU), Law Enforcement Sensitive (LES) scenarios or, perhaps, a set of unclassified scenarios that have an affiliation with classified scenarios. See Figure 4.for a graphic that depicts how access to unclassified scenarios could be layered.

In order to reconcile OPSEC concerns with the desire to adequately meet the existing demand for unclassified scenarios, an online open scenario repository should have different levels of access. In addition, a disclaimer should be included in the repository stating that available scenarios are not official U.S. government documents and do not represent the official position of the U.S. government, unless otherwise stated by the individual scenario. The most logical way to grant access to the repository's

catalog of unclassified scenarios is to categorize each scenario based on its level of sensitivity/classification, and grant access to each category based on users' affiliation with DoD and their "need-to-know" a given category's content. The most permissive category of unclassified scenarios would contain scenarios that are completely unclassified, that is, they are approved for public release regardless of users' "need-to-know" or affiliation with DoD, and thus would be accessible to any and all repository users. The openness of this category would facilitate sharing unclassified scenarios with users outside DoD, for example, international partners, emergency responders and law enforcement officials, interagency partners, and NGO personnel.

The second category of scenarios repository users would have access to are scenarios that have classifications above Unclassified, but below SECRET. This category would include scenarios marked, for example, FOUO, or SBU. Users would be granted access to these scenarios on a limited basis, if they could demonstrate a verifiable "need-to-know" their content and prove that they have a relevant affiliation with DoD.

The third and most exclusive category of unclassified scenarios in the repository would be scenarios that have developer/owner defined "special restrictions." Some unclassified scenario developers/owners may want their scenarios released only to a particular community of the repository's users. These scenarios would not be made available to any and all repository users and would be classified as restricted access only – requiring users to demonstrate a third party approved "need-to-know" and a relevant affiliation with DoD. Furthermore, the users requesting access to scenarios in this category of scenarios would require approval from the scenario's developers/owners. In the online repository, if a user saw a listing of specially restricted scenarios as a result of a search, s/he should be able to click on the scenario and see a dialogue box which prompts users to complete a form requesting access to the scenario. Once completed, the form would be sent electronically to the scenario's developers/owners for review. The scenario developers/owners would decide whether or not the user should be granted access to the scenario in question, based on the validity of the user-provided reason for her/his "need-to-know" and/or her/his affiliation with DoD.
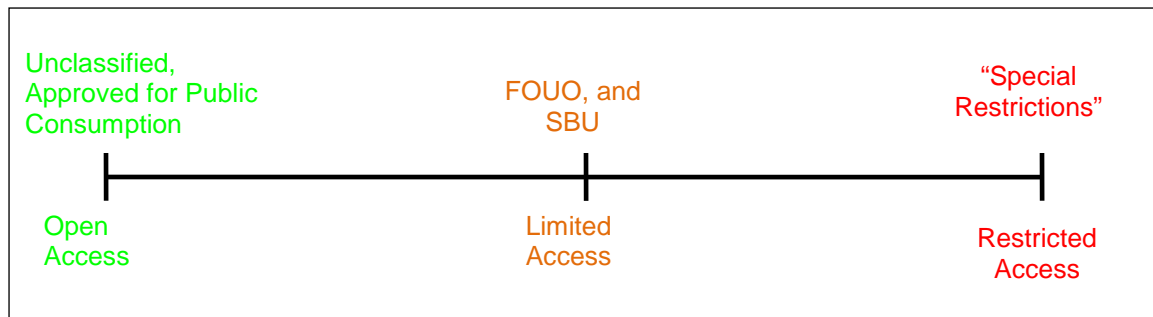
Figure 4. Layered Access to the Unclassified Scenario Repository

Each scenario in the repository would be grouped into one of three categories of unclassified scenarios depending upon their classification. Each scenario level would then be designated as requiring a different level of access based on any given user's "need-to-know" that category's content and their affiliation with DoD.

Different levels of access to scenarios would require a number of screening criteria to be applied to potential repository users in order to determine which unclassified scenarios they would be able to access.[22] These criteria are used to answer two fundamental questions regarding repository access: does the potential user have a "need-to-know" the content of a given category of scenario, and does that individual have a legitimate affiliation (contractor, government employee, etc) with DoD? Which scenarios a potential user has access to would be contingent upon the sufficiency of the answers to these questions. These details would also allow the repository owner(s), and in some instances the scenario developers/owners, to make a judgment on whether or not the potential user has a legitimate "need-to-know" with regards to a scenario's content and decide if s/he has an affiliation with DoD. If answers to these two questions are acceptable and verifiable, the repository owner(s) would then send a password to the user's listed e-mail address, allowing the user to modify the password and create a username and gain access to one or several categories of scenarios.

Additionally, even if the repository were a completely open access site, the repository manager's should require that *all* users at least complete a basic registration form in order to gain access to the repository, if for nothing more than bookkeeping and demographic purposes. Even if the first tier of scenarios are accessible to all repository

---

22 It is recommended that, if for nothing more than bookkeeping and demographic purposes, the repository manager's require *all* users to at least complete a basic registration form in order to gain access to the repository. While the first tier of scenarios may be accessible to all repository users, it would, at the very least, be useful to keep tabs on who is accessing that tier in order to better meet the needs of the repository's customers.

users, it would, at the very least, be useful to keep tabs on who is accessing that tier in order to better meet the needs of the repository's customers. Access to these scenarios would be closely controlled by the repository's managers and would be categorized as having special developer/owner defined restrictions.[23]

<div style="border:1px solid black; padding:10px;">

Additional Option: Categorizing Unclassified Scenarios' Affiliation with Classified Scenarios

As an addendum to the highest, most exclusive, category of unclassified scenarios in the repository, it would be possible to create a classified concordance between any number of unclassified scenarios and classified Defense Planning Scenarios (DPSs) and/or Multi-Service Force Deployments (MSFDs). This could be done with a classified memo promulgated by the Office of the Secretary of Defense (OSD) and the Joint Staff entities responsible for the development of classified DPSs and MSFDs, most notably OSD(P) and the Joint Staff (J8). The memo would highlight which unclassified scenarios were affiliated with a given classified DPS/MSFD and would only be accessible to individuals holding a SECRET security clearance and a demonstrated "need-to-know." Any mention or discussion of the repository's unclassified scenarios having a relationship to a classified DPS/MSFD, in any context, would occur at the SECRET level. For example, equating the U.S. Army's unclassified Multi-Level Scenario 1.0 (MLS 1.0) to OSD's classified Conventional Conflict-2 (CC-2), even through the use of the unclassified codeword's "MLS 1.0" and "CC-2" would be classified as a SECRET level discussion.[24]

</div>

Recommended Action: Grant access to the repository's content by grouping scenarios into different categories based on each scenario's classification. The first category of scenarios would include scenarios that are unclassified and approved for public release. Any and all repository users would have access to these scenarios. The second category of scenarios would be scenarios marked as For Official Use Only, Sensitive But Unclassified, etc. Access to these scenarios would require users to demonstrate a "need-to-know" for their content and an appropriate affiliation with DoD. The third category of scenarios would include scenarios that have specific developer/owner defined special restrictions. For these scenarios, access would be granted to users by each scenario's

---

[23] IDA has not assessed whether or not there is a demand for unclassified scenarios that have a linkage to classified DPSs/MSFDs. IDA is simply positing an option that could be used should repository users' demand, after the construction of an online unclassified scenario repository, a set of unclassified scenarios that have a linkage to DPSs/MSFDs.

[24] There is no real-world affiliation between the U.S. Army's unclassified MLS 1.0 and OSD's classified CC-2 scenarios. This example is purely illustrative.

developers/owners on a case-by-case basis and would likely require users to demonstrate a relevant "need-to-know" and an appropriate affiliation with DoD.

The repository's managers should annually review which category of scenarios users have access to and "re-certify" each user's access to a given category.

b. Including Scenarios in the Repository: A Tiered Approach

To satisfy as much demand for unclassified scenarios as possible, it would be ideal to include as many unclassified scenarios in the repository as practical, regardless of their structure or level of detail. Phase One of the Open Scenario Study and the compilation of unclassified scenarios during the construction of IDA's Open Scenario Repository beta site have informed the IDA study team that unclassified scenarios of many different styles and structures exist. These styles and structures are largely determined by the number of scenario "components" used to build the scenario and the level of detail scenario developers provided for each component. Phase One also identified seven major components of a scenario and uncovered overwhelming concurrence from the national security community regarding their importance to the construction of both classified and unclassified scenarios. The seven components are: assumptions, context/road to war, threat/challenge, objectives, strategic concept, concept of operations, and forces data.[25] As information to users, the repository should note which of these components each scenario in the repository has, so users can more easily find scenarios that meet their specific needs.

One of the potential benefits of admitting as many scenarios as possible into an online unclassified-scenario repository is that doing so allows users to find scenarios to satisfy their specific scenario needs and to conduct a variety of different analyses. While some repository users may need highly detailed scenarios in order to run specific modeling and simulation applications, others may need less detailed challenges in order to explore strategic-level concepts of operations. Because of this discrepancy between varied user needs, an online unclassified scenario repository may need to house hundreds, if not thousands, of scenarios that differ in the number of components used to build the scenario and their level of detail. Including as many scenarios as possible would also ensure that unclassified scenario users have access to scenarios that completely cover the traditional, irregular, disruptive, and catastrophic challenge spaces and will go a long way

---

25 *Open Scenario Study, Phase I, Volume 1: Assessment Overview and Results* (IDA Paper P-4326), p. 63.

towards meeting the national security community's demand for unclassified scenarios. However, as the repository evolves and matures over time, it is possible that scenarios included in the repository may become outdated and actually degrade the value of content and/or make searching processes more difficult. Thus, it would also make sense to periodically "purge" the repository of obviously outdated content.

Recommended Action: Include as many unclassified scenarios in the repository as possible. As information to users, note which, if any, scenario components (assumptions, context/road to war, threat/challenge, objectives, strategic concept, concept of operations, and force data) a given scenario has and its level of detail. Additionally, the repository managers should occasionally purge the repository of content that is obviously outdated or irrelevant.

3. Housing an Online Unclassified Scenario Repository

An additional measure that can be taken to help alleviate OPSEC concerns is to link the repository's access point to an official DoD website.   By doing so, the repository's government owner(s) would be able to monitor the traffic in and out of the website and require users to acknowledge that they may be monitored during their activities.   For example, the unclassified Joint Data Support website has the following disclaimer users must agree to before entering the site:[26]

> "You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only. By using this IS, you consent to the following conditions:
>
> - The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations.
>
> - At any time, the USG may inspect and/or seize data stored on this IS and any device attached to this IS.
>
> - Communications occurring on or data stored on this IS, or any device attached to this IS, are not private.   They are subject to routine monitoring and search.
> - Any communications occurring on or data stored on this IS, or any device attached to this IS, may be disclosed or used for any USG-authorized purpose.

---

[26]   The online Joint Data Support website at https://jds.pae.osd.mil/Default.aspx: accessed January 28, 2010.

- Security protections may be utilized on this IS to protect certain interests that are important to the USG. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the USG. These protections are not provided for your benefit or privacy and may be modified or eliminated at the USG's discretion."

This disclaimer might serve not only as a deterrent to the repository's unintended audience, but would also allow the manager(s) and/or owner(s) to monitor the traffic in and out of the website and repository, more so than if the repository were stored on a standalone website.

Recommended Action: House the repository on an official DoD website, so that the repository's manager(s) and/or owner(s) can monitor the traffic in and out of the repository. Also, before a user can access the repository, present him with a disclaimer requiring his consent to monitoring and compliance with all official U.S. government and DoD information system policies and procedures.

D. OWNERSHIP AND MANAGEMENT

In order to make sure the online unclassified scenario repository receives the guidance and stewardship necessary for making it a viable and useful approach for meeting the national security community's demand for unclassified scenarios, a DoD entity will need to take ownership of the repository and provide it with a full-time, authoritative management apparatus.

This management body, which would require support from its principals, would be given the authority necessary to successfully build and maintain IDA's recommended approach. Without such support, and authority, it's unlikely that sufficient resources or attention would be allocated for the successful execution of IDA's recommended approach.

The repository owners and managers need not be newly created entities. Instead, an existing joint DoD governing body could be used or modified in order to provide guidance and oversight for the online unclassified scenario repository. An example of such an entity is the Modeling and Simulation Integrated Process Team (M&S IPT). This team represents a broad cross-section of different DoD organizations involved with modeling and simulation and consists of personnel from DoD's acquisition, analysis, planning, testing, training, and experimentation communities.[27] Because of the broad

---

27 The M&S IPT has representatives from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD [AT&L]), the Office of the Under Secretary of Defense, Personnel and Readiness (OUSD [P&R]), the Office of the Director for Cost Assessment and Program

representation on the M&S IPT and its mission to provide oversight for a number of analytic activities that involve scenarios, both unclassified and classified, it would be uniquely suited for providing the online unclassified scenario repository with the necessary strategic guidance and oversight. Additionally, the broad list of organizations on the M&S IPT *roughly* represents the functional activities performed by the unclassified scenario user communities identified by IDA in Phase One of the Open Scenario Study. Using the M&S IPT would enable these disparate unclassified scenario user communities to become aware of each other, if they are not already, and collaborate.

The M&S IPT would meet periodically (weekly, monthly, annually, as needed, etc.) in order to provide the repository's day-to-day managers with official guidance and direction. While the managers would take care of the daily responsibilities of the repository, such as posting scenarios, technical and maintenance issues, granting admission to potential repository users, and responding to user inquiries, the M&S IPT's purpose would not be much different from its current role as the modeling and simulation community's analytic governing body. As the repository's owner, the M&S IPT would give the managers overarching strategic direction on issues such as the criteria that are applied for granting a user admission to the repository's tiers of scenarios, the expenditure of allotted funds, the nomination and approval of the management team's leadership, which would likely consist of DoD personnel whose principals are on the M&S IPT, the approval of new repository functions (e.g., a blog), etc. Additionally, the M&S IPT would also be required to resolve issues that the repository's managers request guidance on, perhaps by way of voting.

Despite the fact that the M&S IPT is a DoD entity, DoD should *not* be solely responsible for providing strategic guidance to the repository's managers. As previous sections of this report have advocated, unclassified scenario products should be available to the broader interagency community, which would help remove barriers that have impeded collaborative efforts in the past. The utilization of an open scenario repository by the U.S. Department of State (DoS), and other related organizations with an

Evaluation (OSD [CAPE]), the Office of the Under Secretary of Defense for Intelligence (OUSD [I]), the Office of the Director, Operational Test and Evaluation Directorate (DOT&E), the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD [NII]), the Office of the Under Secretary of Defense for Policy (OUSD[Policy]),the U.S. Army, the U.S. Navy, the U.S. Air Force, the U.S. Marine Corps, U.S. Joint Forces Command (USJFCOM), the Joint Staff's Directorate for Operational Plans and Joint Force Development (Joint Staff [J7]), and the Joint Staff's Force Structure, Resources, and Assessment Directorate (Joint Staff [J8]). The M&S IPT is chaired by the representatives from OUSD(AT&L) and is tasked with providing oversight and guidance to much of DoD's analytic work that results from modeling and simulation.

international focus, for example, could effectively leverage scenarios involving its DoD counterpart to ensure a more holistic approach to accomplishing U.S. diplomatic objectives. Additionally, since any number of the scenarios in the repository may be non-DoD products, and since there is a large demand for unclassified scenarios among DoD's partners, the M&S IPT's expertise and guidance would be greatly enhanced by including personnel from some of DoD's major interagency partners; for example, DoS, Department of Homeland Security (DHS) and/or the Federal Emergency Management Agency (FEMA). Because many of DoD's partner organizations would have a vested interest in the repository's content and functionality, it would be particularly beneficial for the M&S IPT to leverage the scenario expertise and "best practices" of other organizations. This could lead to the inclusion of personnel from other governmental and non-governmental partner organizations to form an "M&S IPT-plus" ownership body. A M&S IPT-plus ownership body would not only strengthen the strategic guidance issued to the repository managers and ensure that the broader interests of non-DoD repository's major stakeholders are represented, but would also enhance existing relationships between DoD and its partners in the realm of scenario development and use.

Recommended Action: OSD should designate a joint organization, such as DoD's Modeling and Simulation Integrated Process Team (M&S IPT), as the owners of the online unclassified scenario repository. The M&S IPT's primary function would be to provide guidance for and oversight over the repository. However, because many of DoD's interagency and non-governmental partners also have a vested interest in the direction and content of the repository, it would be beneficial to consider their input and leverage their scenario expertise. This would mean the modification of the M&S IPT into a "M&S IPT-plus" ownership group that includes DoD's partners (e.g., DoS, DHS, FEMA, etc.) in the world of repository development and oversight. The M&S IPT-plus would issue strategic guidance to the repository's day-to-day managers and the decision-making bodies designated by individual unclassified scenario user communities (explained in detail in the next section), have control over the repository's budget, and would resolve any strategic issues brought forth by the managers. The repository's managers would consist of DoD (and possibly non-DoD) personnel whose principals are members of the M&S IPT-plus ownership group.

E. BUILDING COMPLETE SETS OF UNCLASSIFIED SCENARIOS – USER-DEFINED UNCLASSIFIED SCENARIO NEEDS

While the repository may likely contain hundreds, if not thousands, of unclassified scenarios, it would be useful to include preferred sets of unclassified

scenarios that have preferred standing in the various scenario user communities. Using the ideas outlined in Chapter III., which discusses certifying scenarios as an indication of organizational preference, having user community-specific, preferred sets of unclassified scenarios would allow repository users to have a common baseline from which to begin their studies and analyses, allowing for comparability of results, while also lending an element of credibility to analytic work within their community. Additionally, including preferred sets of unclassified scenarios in the repository would also help meet user community-specific demands for unclassified scenarios.

The creation of preferred sets of unclassified scenarios would require the recognition of sub-sets of unclassified scenarios in the repository as being preferred by a given organization, in this case a particular scenario user community. User community designation of preferred sets of unclassified scenarios is preferable to a universal, M&S IPT-plus defined set of "official" unclassified scenarios because user communities have diverse needs for unclassified scenarios that likely cannot be satisfied by a single set. For example, one user community could decide that a given complete set of scenarios needs to be usable for a range of analytic activities, while another decides that their complete set needs to cover certain geographical areas of the world.

The creation of these sets would be similar to section 2.b. entitled "Certification as Organizational Preference," which is discussed in Chapter III. Element Two. As explained in Phase One and in previous sections of this report, the demand for unclassified scenarios is not monolithic in the sense that various communities of unclassified scenario users need scenarios for different activities and organizational functions. Rather, it is unlikely that a single, certified set of unclassified scenarios would meet the varying aspects of users' demand for unclassified scenarios. The best strategy to reconcile the *differences* in need with the overarching fact that there *is* a need for unclassified scenarios is to let various communities of unclassified scenario users define, among themselves, what constitutes a certified set of unclassified scenarios.

To help procure complete sets of unclassified scenarios for inclusion in the repository, the M&S IPT-plus should encourage individual user communities to develop Community Working Groups (CWGs) that define what their community prefers in a certified set of unclassified scenarios and assist the CWGs in promulgating scenarios to complete their sets. This method leverages the expertise of those who know their requirements for unclassified scenarios best which would help satisfy user communities' diverse needs for unclassified scenarios.

As Phase One of the Open Scenario Study indicated, a great deal of time and effort has already been invested in the development of unclassified scenarios. In order to leverage others' investment in time and resources, both human and capital, the M&S IPT-plus should attempt to compile user-defined sets of unclassified scenarios by making use of the unclassified scenarios that are already in existence. This would necessitate a DoD-wide mandate, perhaps in the form of a DoD Directive, requiring all DoD organizations provide copies (either paper or electronic) of their unclassified scenarios to the M&S IPT-plus. While it would be too laborious and time-consuming for M&S IPT-plus to discern which scenarios are appropriate for inclusion in the preferred sets, they could give the CWGs access to the scenarios and let them decide which ones ought to be included in their final sets. This would save the M&S IPT-plus time and effort in deciding which scenarios should be designated as having some level of preference, while simultaneously leveraging the expertise of those who best know their communities' unclassified scenario needs. The user communities would review the unclassified scenarios and submit to the M&S IPT-plus their preferences for which ones ought to be designated as community-preferred scenarios. The M&S IPT-plus would then review the proposals and include the preferred sets in the repository.

While there are likely thousands of unclassified scenarios that would be included in the online unclassified scenario repository, there may be an absence of a scenario, which leaves a "gap" in a given user-defined set of scenarios. For example, upon aggregating and assessing existing unclassified scenarios, a CWG may decide that there are scenarios of sufficient quantity and/or quality covering South American geography, but that a scenario does not exist for Africa. Filling the gap would simply require that the CWGs inform the M&S IPT-plus of a significant need for any unclassified scenario that does not already exist in the online repository, but is needed in their preferred set. It would then be M&S IPT-plus' prerogative and responsibility to facilitate the development of a scenario that fills the identified gap. If a CWG can present a compelling case to the M&S IPT-plus that a gap renders its set incomplete, and the M&S IPT-plus concurs with the CWG's recommendation, then the M&S IPT-plus could task the development of new scenarios to those organizations with relevant scenario-development expertise, and provide them with necessary funding. After the scenario is developed, it would then be included with the other scenarios in that community's preferred set. This idea is similar to the third option, evolving OUSD(P)'s existing DPS enterprise into a distributed organization, discussed Chapter IV. in the analysis of Element Three, but is different in the sense that the organizations tasked by the M&S

IPT-plus with the development of new unclassified scenarios need not mirror the OUSD(P)'s DPS development process.

Recommended Action: Each community of unclassified-scenario users should be required to create a community working group (CWG) that defines their community's scenario needs and preferences. The M&S IPT-plus should assist in the development of each community's complete set of preferred unclassified scenarios by issuing a DoD Directive requiring that all DoD entities send copies of their unclassified scenarios to it for review and inclusion in the repository. The M&S IPT-plus should then leverage the expertise of the user CWGs by reviewing their recommendations for what constitutes a complete set of unclassified scenarios for their community. The CWGs would nominate to the M&S IPT-plus specific unclassified scenarios, through an official nomination process, as being of high enough quality to be included in their preferred unclassified scenario set. The M&S IPT-plus would review the nominations and include them in the repository. If a community work group identifies a "gap" in the existing universe of unclassified scenarios and states a case that the gap should be filled, the M&S IPT-plus would task an organization with relevant expertise, perhaps within the community requesting the new scenario, to develop the new scenarios.

VII. CONCLUSION

Phase One of the Open Scenario Study revealed that significant demand exists for unclassified scenarios throughout the national security community.[28] Phase One also uncovered obstacles that prevented those who need unclassified scenarios from accessing the existing universe of unclassified scenarios, leading to duplication of unclassified scenario development efforts and unnecessary resource expenditures. Throughout the course of Phase One, the scenario user community expressed preferences for how DoD might better address the demand for unclassified scenarios. IDA translated these user community preferences into four "elements" that any DoD approach to unclassified scenarios should include:

Element One – online open scenario repository,

Element Two – certification of existing scenarios,

Element Three – development of new a unclassified scenarios set(s), and

Element Four – declassification of (portions of) existing classified scenarios.

In Phase Two of the Open Scenario Study, IDA explored and analyzed these four elements, individually and in combination, and their potential in developing a comprehensive approach that DoD might adopt to address the national security community's demand for unclassified scenarios. The IDA recommends development of an approach to best address the need that exists for the unclassified scenarios.

This chapter conveys the major findings from Phase Two, summarizes the recommendations to DoD, and identifies potential next steps in the process.

A. MAJOR FINDINGS

Four major findings emerged from Phase Two of the Open Scenario Study:

---

[28] *Open Scenario Study, Phase I, Volume I: Assessment Overview and Results* (IDA Paper-P 4326), March 2008.

1. Few, if any, organizations have awareness and access to the universe of unclassified scenarios developed and used by DoD and its interagency partners.

One of the main impediments in meeting the demand for unclassified scenarios is awareness and accessibility to unclassified scenarios. The development and employment of an online open scenario repository would help make existing unclassified scenarios available to those who need them. Access to the Internet would be the only technical requirement that scenario users would need in order to gain access to the online repository. However, the owners of the repository would decide on the various ways users could access the repository and the level of restrictions it will have. An online open scenario repository could offer different ways to access scenarios. As the demand for unclassified scenario is also strong outside of DoD, the online open repository would enable other government agencies, NGOs, allied nations and private-sector organizations to gain access and use unclassified scenarios for their needs as well.

2. DoD would benefit from promoting the reusability of unclassified scenarios.

The development of unclassified scenarios is ongoing throughout the DoD. These efforts are often times not integrated with DoD-wide processes, nor widely coordinated among DoD's diverse base of interagency partners as other government agencies and organizations are also involved in developing their own unclassified scenarios. The reuse of existing scenarios could result in reducing unnecessary duplication of efforts, help maximize cost-savings, increase DoD- and government-wide knowledge sharing and best practices as well as improved interagency collaboration and coordination. Therefore, DoD's unclassified scenarios along with similarly qualified non-DoD unclassified scenarios could populate a portion of a future set of unclassified scenarios and would allow for usage to other government agencies and services. Creating a "one-stop-shop" would further afford increased efficiencies and improve productivity, as well as promote greater commonality, collaboration and integration of related scenario development and implementation practices.

3. The U.S. Army's unclassified Multi-Level Scenario (MLS) framework provides a potential foundation for joint unclassified scenarios development and use.

As noted earlier, the development of unclassified scenarios is ongoing throughout the national security community. Within the DoD, specifically the U.S. Army's Multi-Level Scenario (MLS) provides an example of an existing codified and institutionalized

process that could be utilized and leveraged while developing an approach model. The MLS is a useful tool as it provides a similar structure to the DPS-derived scenarios but avoids issues of classifications and life span. The MLS has greater flexibility to adjust and meet the needs of a broader audience of unclassified scenarios. The IDA study team noted that the MLS's disadvantage is that it is Army-centric and other Services are not actively participating in the development process; however, opportunities exist for joint participation.[29] Furthermore, if other Services are included in the MLS development process, an organization in the modeling and simulation could provide guidance to elevate the scenario(s) for DoD-wide use and it could create a potential foundation for joint unclassified scenarios.

4. Unclassified scenario development and use provides a unique opportunity to strengthen interagency collaboration and coordination.

In recent years, IDA has noticed a blurring of lines in roles and responsibilities between civilian and military organizations due to the complexity and overlapping of challenges and threats facing the U.S. The appropriate mix of civilian and military operations has become vital to the U.S. strategic national security planning efforts. Domestically, the roles of several civilian agencies (DoS, DHS) are often analogous to, and oftentimes commensurate with, DoD. Similarly, U.S. civilian agencies working abroad are collaborating with the U.S. military to support reconstruction and stabilization operations (for example, Office of the Coordinator for Reconstruction and Stabilization (S/CRS) at DoS). The successful outcome of these operations depends largely on the effectiveness of their coordination and collaboration. Both civilian and military agencies utilize scenarios and exercises but there is lack of a common platform to create the collaborative linkages. Development of an online open repository and providing access to [all] other government agencies would improve interagency collaboration and coordination. As noted in the Phase One report, "permitting participation of those organizations lacking clearance" would be an important driver in the use of unclassified scenarios. The unclassified nature of these scenarios would remove OPSEC concerns that have impeded joint efforts in the past. This "whole-of-government" approach to the online open scenario repository could initiate the creation of a platform for future joint planning and training for civilian-military operations. The unclassified and open nature of the repository and its scenarios could encourage international participants such as allies and humanitarian organizations to use the scenarios to determine how to better

---

[29]   *Open Scenario Study: U.S. Army's Multi-Level Scenario Sub-Task* (IDA Paper P-4466).

integrate their roles and responsibilities in various domestic and international operations consistent with U.S. goals.

B. FOUR ELEMENTS OF AN APPROACH

In the Phase One report of the Open Scenario Study, the unclassified scenario user community provided perspectives on how they use scenarios and how the process for developing and sharing scenarios might be improved. In Phase Two of the study, these preferences were translated by the IDA study team into four distinct "elements" that should be considered by DoD if it wants to address the identified demand for scenarios. These elements were then analyzed in detail to determine their potential usage in developing a recommended approach for the Department. IDA determined that a combination of these elements in developing an approach could ensure the widest number of users access to the unclassified scenarios.

The following are the key features of the four elements of an approach that were evaluated by the IDA study team:

Element One: Online Open Scenario Repository

Description of the Element: An online searchable database of unclassified scenarios developed by any source. Such a database has the ability to reach the largest audience of unclassified scenario developers and users.

Key considerations in this element include:

- Degree of user access developed by the repository's owners and managers.

- Standards for user access decided by the repository's owners and managers.

- Criteria for the inclusion of scenarios decided by the repository's owners and managers.

- Management system required to maintain and update the repository.

- Method of distribution that makes scenarios available for download or links users to secondary third party sources.

- Ability to search and browse the content easily.

- Rating system that would allow users to score how useful the repository's scenarios are.

- Communication between users and repository's managers can be done either through blogs and/or message boards and it would help improve the system and stimulate collaboration.

- Wiki can enable users to post their scenarios themselves or to alter pre-existing scenarios.

- Costs of maintaining and managing could depend on the size and degree of functionality of the repository.

Element Two: Certification of Existing Scenarios

Description of the Element: Designation of a pre-existing set of unclassified scenarios as "preferred" for use throughout the community of unclassified scenario users. The quality and characteristics differ widely among the unclassified scenarios from disparate sources. A certification process would be required to meet a set of common standards and rules.

In Phase Two, IDA evaluated two types of standards that could be used to qualify a scenario for certification:

- Certification as information for users would be geared toward noting the presence of various scenario elements in a scenario but, not rating the quality of those elements.

- Certification as an organizational or community-wide preference would use different criteria and would be tailored to the purpose of the certifying organization. The standards for this certification would address more directly the content of scenarios and include various considerations about the scenario.

Element Three: Development of a New Unclassified Scenario Set

Description of the Element: Development and maintenance of a new set of unclassified scenarios akin to classified DPSs. OUSD(P)'s existing DPS process is a codified and institutionalized method of producing and distributing DoD's official set of classified scenarios. The DPS process and products enjoy authority throughout DoD and among several of its external partners.

There are four organizational concepts for producing new unclassified (DPS-like) scenarios evaluated by the IDA study team in Phase Two:

- Expand OUSD(P)'s existing DPS enterprise by leveraging its existing capabilities and expand them to produce official unclassified scenarios.

- Create a parallel (but independent) DPS enterprise for unclassified scenarios by replicating OUSD(P)'s existing model and reconstituting it within a newly formed and independent organization.

- Evolve OUSD(P)'s existing DPS enterprise into a distributed organization by incorporating benefits of the first option while making use of DoD's ad hoc and decentralized unclassified scenario development capacity.

- Outsource unclassified scenario functions to the private sector while incorporating relevant aspects of the three concepts above with notable exception of outsourcing the bulk of DoD's future capabilities in unclassified scenarios to the private sector.

Element Four: Declassification of Classified Scenarios

Description of the Element: Identification and removal of sensitive materials in classified DPSs to produce an official sanitized set of unclassified scenarios.

When examining Element Four, IDA identified three challenges which would produce costs that outweigh the benefits of declassifying classified scenarios, and so eliminated the element from being considered as part of an approach designed to meet the demand for unclassified scenarios. The identified challenges are:

- Determining which unclassified scenarios would benefit the DoD community and which classified data must be replaced with open source data to keep the scenario viable for unclassified use would be a difficult and time consuming task.

- Many DPSs would lose their inherent value when stripped of classified operating environments and depictions of U.S. capabilities.

- U.S. adversaries may be able to deduce depictions of classified U.S. military capabilities through the aggregation of unclassified data.

C. IDA'S RECOMMENDED APPROACH

The four desired elements outlined above could produce a number of combinations of approaches resulting in an approach that DoD could implement. First, each element was examined as a standalone approach based on the application of three selection criteria, which eliminated the possibility of any element alone being sufficient. The selection criteria were:

- Availability: availability of the approach to the largest possible audience of unclassified scenario users,

- Flexibility: ease with which changes in scenario content can be made available to the community of unclassified scenario users, and

- Responsiveness: responsiveness to varying aspects of unclassified scenario users' demand for unclassified scenarios.

In Chapter VI., four combinations of these elements were presented after it had been determined that no single element alone would suffice as an approach to meeting the demand for unclassified scenarios. IDA recommends using an approach that would include a permutation of three individual elements. The recommended approach would certify, as an indication of individual communities of unclassified scenario users' preference, existing unclassified scenarios (Element Two) and develop new scenarios (Element Three), as needed, to create an official set of scenarios that is housed in an online repository (Element One). Furthermore, the proposed approach includes the following key features:[30]

- An online unclassified scenario repository. The online repository should be a summary database equipped with both basic search capabilities and advanced search functions that provides in-depth search capabilities. The repository should also have the necessary tools (blogs, message boards, and wikis) for the users and owners to communicate with each other effectively and help improve the site's functionality and content as well as promote future collaboration. Access to the repository content should be granted by grouping the scenarios into different categories based on each scenario's classification. Additionally, the repository should include as many unclassified scenarios as possible and the repository should be housed on an official DoD website, so that the repository manager can monitor traffic to the site.

- OSD should designate a joint organization, such as DoD's Modeling and Simulation Integrated Process Team (M&S IPT), as the owners of the online unclassified scenario repository. The M&S IPT is well suited as the owners of the repository due to the fact that it roughly comprised of and represents the functional activities of individual unclassified scenario user communities. The primary function of M&S IPT would be to provide guidance for and

---

[30] See Chapter VI. of this report for a detailed discussion of the recommended approach.

oversight for the repository. Including other government agencies (e.g., DOS, FEMA, and DHS) would permit consideration of their needs because of interagency and civil-military operations. Inclusion would also allow for leveraging of their respective expertise in scenario development and presentation.

- Each community of unclassified-scenario users should be required to create a community working group (CWG) that defines their scenario needs and preferences by certifying existing unclassified. M&S IPT-plus (an ownership body that includes DoD and other government agencies) should issue a DoD directive requiring all DoD entities send copies of their unclassified scenarios to it for review and inclusion in the repository. Any additional needs for unclassified scenarios identified by CWGs will be tasked for development by the M&S IPT-plus.

The proposed approach was chosen because of the following reasons:

- An online repository would reach the widest audience possible, ensuring unclassified scenario demand could be met.

- Changes in unclassified scenario content would be made readily available to the community of unclassified scenario users.

- The approach would be responsive to the various aspects of unclassified scenario users' demand for unclassified scenarios.

- Large numbers of unclassified scenarios would be easily stored and searchable.

- Leveraging existing scenarios would reduce duplication of unclassified scenario development efforts and associated expenditures, and would increase the diversity and depth of scenario efforts.

- This approach maximizes opportunities to increase collaboration between DoD and its major external partners.

D. NEXT STEPS

As Phase One of the Open Scenario Study revealed, there is a strong demand throughout the national security community for unclassified scenarios. [31]   An

---

[31] *Open Scenario Study, Phase I, Volume I: Assessment Overview and Results* (IDA Paper-P 4326).

overwhelming majority of those interviewed/surveyed during Phase One said they would use unclassified scenarios more if they were made more readily available.[32]

Phase One also identified user preferences for and insights into the characteristics of an approach for better satisfying the community's need for unclassified scenarios. In Phase Two, based on these insights and preferences, IDA evaluated possible approaches that could be used to meet the demand for unclassified scenarios.

The IDA study team developed a tailored approach that best addresses the community's need for unclassified scenarios as demonstrated by Phase One of the study. IDA's recommended approach includes an online repository (Element One) – a leading preference identified in Phase One among those who need unclassified scenarios for their work – as its foundation. The recommended approach does not consider declassifying classified scenarios (Element Four) as a feasible aspect of the solution, a process which IDA estimated to be difficult while making few, if any, contributions to an approach used to satisfy unclassified scenario demand. The recommended approach also suggests leveraging existing unclassified scenarios by certifying (Element Two) and including them as part of a preferred set (Element Three), should they meet a pre-designated set of criteria set forth by individual unclassified scenario user communities.

The combination of these elements would ensure access to the widest audience of unclassified scenario developers and users.

Lastly, the involvement of DoD's senior management would ensure that adequate resources and priority are allocated to the successful implementation of the recommended approach. Without the attention and authority of the Department's relevant senior managers, it is unlikely that the recommended approach would be executed to the extent required to meet the demand for unclassified scenarios. Prior to implementing IDA's recommended approach, the Department should consider the following next steps:

- **Determine the costs to build and maintain the repository.**

Once a government decision is made to develop an online open scenario repository with the features this report describes, a necessary step would involve analyzing the costs for maintaining this enterprise.

- **Design a management scheme and ownership of the repository.**

---

[32] Based on Phase One surveys and interview results, when asked if they would use unclassified scenarios more often if they were more readily available to them, sixty-one percent of questionnaire respondents noted that they would use unclassified scenarios to complete their task.

Important in the process would be to decide who owns the repository and the management scheme used to run it. In Phase Two, the IDA study team analyzed the infrastructure that exists within DoD regarding the scenarios set, and recommended a few organizational/ownership concepts for producing new unclassified scenarios. The next steps would require more detailed discussions and recommendations regarding the ownership models. The need for unclassified scenarios will only be met when there is an ownership model in place that ensures the widest access possible to the repository of unclassified scenario sets.

Similarly, a management scheme needs to be designed that would operate the repository. In the Phase Two report, the IDA study team explored a few models that could ensure the widest participation possible of the community users but in the next steps more detailed recommendations need to be designed regarding the management scheme.

- **Design a new process for the development of the unclassified scenarios.**

Before employing IDA's recommended approach, providing a detailed schematic of the aforementioned unclassified scenario development process would be necessary.

- **Launch a campaign to promote the repository.**

The goal of developing an online open repository is to reach the widest possible audience and encourage the greatest number of relevant users. The owners should ensure the information for development of such a repository is promulgated extensively and an aggressive marketing campaign is employed for these reasons.

- **Create individual unclassified scenario user community working groups to oversee the process of certifying existing unclassified scenarios.**

The existence of unclassified scenarios among different government institutions and the use of these scenarios in an approach designed to meet the demand for unclassified scenarios places an important role on the certification process. Therefore, certification of existing unclassified scenarios would require the creation of a central body, by each community of unclassified scenario users, which would design standards, rules and regulations for such a process.

In summary, Phase Two of the Open Scenario Study analyzed four elements, individually and in combination with one another, that could be used to build an approach for addressing the national security community's demand for unclassified scenarios. The approach proposed here, if implemented by DoD, would promote widespread reuse of

unclassified scenarios by DoD and its key partners. Implementing the proposed approach would be cost-efficient, reduce redundancy, and improve interagency collaboration and cooperation.

APPENDIX A:
SUMMARY OF PHASE ONE REPORT

A. BACKGROUND

Scenarios are widespread throughout DoD, and they serve a variety of functions. In recent years, the Department has made significant progress in developing and coordinating a common set of classified scenarios, but it has no similar process for unclassified scenarios. Because of this gap, DoD and its partners have undertaken disparate efforts that have frequently produced incomparable and redundant unclassified scenarios. To examine this situation and develop potential solutions to better address the need for unclassified scenarios, DoD asked IDA to conduct a study of unclassified scenario development and use in the Department and among key DoD partners.

B. APPROACH

The overall study design includes three phases: (1) assessment of unclassified scenario needs, (2) development and assessment of approaches for satisfying these needs, and (3) further development of the selected approach. This report conveys the results of phase one of the study.

Phase One encompassed a multifaceted approach to assess the need for unclassified scenarios among DoD users and their partners. The first step of Phase One included problem definition and scoping through engagement with key stakeholders. An extensive literature review of both DoD and non-DoD sources was the second step. The third step involved surveying the national security community to gain insights and perspectives. This was done through an extensive questionnaire and selected interviews. The community surveyed included the Office of the Secretary of Defense, Joint Staff, Military Services, Combatant Commands, military and civilian educational institutions, U.S. interagency, foreign partners, defense industry, and other select organizations (federally-funded research and development centers, DoD agencies, etc.).

C. KEY FINDINGS

Analysis of the results from IDA's Phase One approach yielded several major findings:

1. **Scenarios are important to most of the national security community.** Over ninety percent of the organizations surveyed found both classified and unclassified scenarios important to the functions they performed.

2. **Strong demand for unclassified scenarios exists.** Almost forty percent of the community indicated that unclassified scenarios were "very important" and sixty percent indicated that they would make more use of them if more were available.

3. **Scenario development imposes significant recurring costs but potential for major cost-savings exists.** Of the group surveyed, scenario development costs over $80 million annually ($30 million for unclassified and $50 million for classified). They estimated that potential unclassified scenario approaches could save over $10 million annually.

4. **Several factors drive use of unclassified scenarios.** There are real requirements that create the need for unclassified scenarios. The leading drivers are: (1) permitting participation of those organizations lacking clearances, (2) ease or convenience of use and handling, (3) lack of compelling need for classified scenarios, (4) perceived inflexibility of classified scenario data.

5. **Some commonality in scenario definition and form exists.** Across DoD and its partners, there was substantial agreement on the basic form and definition of scenarios. Almost eighty percent of respondents generally agreed with a definition that was provided. A majority felt that the following were "very important" components of scenarios: threat/challenge, concept of operations, assumptions, objectives, forces data, and strategic concept.

6. **Current classified scenario products (e.g., Defense Planning Scenarios) appear to meet needs well, with some suggestions for enhancement.** Over sixty percent of respondents indicated that current or planned classified scenario products satisfied their organizations' needs for classified scenarios. Some suggestions included increasing the number of long-term scenarios and developing a broader array of challenges.

7. **Potential approaches exist for better satisfying unclassified scenario need.** Several approaches provided were judged to offer cost-savings; other promising options were offered by respondents and interviewees themselves.

APPENDIX B
ANALYTIC AGENDA BACKGROUND

This appendix is an adaptation of Appendix C of the IDA Paper entitled *Improving Integration of Department of Defense Processes for Capabilities Development Planning*, (P-4154) by John T. Hanley, et al., September 2006.

DoD's Analytic Agenda is a set of activities designed to accomplish the following four objectives:

- Articulate, through scenarios, the Secretary of Defense's guidance to DoD about the missions, environments, and threats for which the future force should be prepared;

- Apply joint concepts to future missions depicted in planning scenarios;

- Produce standardized, accessible, transparent data and common assumptions for Department-wide use in analysis;

- Design and conduct major joint analyses to support decisions on force structure, investments, and capability trade-offs.

Defense Planning Scenarios (DPSs) are part of the Secretary's guidance to the Department on capabilities development planning and programming. They are the starting point for analyses supporting the Planning, Programming, Budgeting and Execution (PPBE) process, the Quadrennial Defense Review, and other major defense planning efforts. Each DPS depicts a specific hypothetical operational challenge that might be faced by the future force. Together, all DPSs are meant to address a full range of major military operations. DPSs are produced for two future timeframes, nominally the "mid-term" (Future Year Defense Program +1) and the "long-range" (Future Year Defense Program +13). In this way, DoD's Analytic Agenda provides guidance and data for analyses supporting decisions that affect plans and programs that span both of these timeframes. The major steps of DPS development are as follows:

- Scenario selection

- Drafting of scenario framework, assumptions, variables

- Drafting of threat description and adversary concept of operations (CONOPS)

- Drafting of a U.S. strategic concept for addressing the scenario challenges

- Integration and coordination of complete scenario draft.

One DPS is unique and merits special description. The Steady State Security Posture / Integrated Security Posture (SSSP/ISP) depicts overall global force posture rather than a single hypothetical challenge. In addition to projected overseas basing of forces, the SSSP depicts a number of representative lesser contingencies (e.g., humanitarian assistance, foreign internal defense, etc.) and ongoing operations (e.g., homeland defense surveillance, exercises, etc.). The purpose of the SSSP is to provide an estimate for the steady-state demand on forces and, with its ISP component, to establish a framework for analytically combining the demands from different combinations of simultaneous scenarios.

Analytic Agenda scenarios and data are intended to provide the basis for analyses throughout DoD, especially in such venues as Joint Capabilities Integration and Development System (JCIDS) Capabilities-Based Assessment (CBAs). Component analyses conducted to support programming decisions are expected to use Analytic Agenda scenario and data products as a "starting point." Also, the results of joint analyses conducted under the Analytic Agenda should inform future planning and priorities for concept development and experimentation. In particular, useful lessons for future concept development and experimentation may be derived from the application of joint concepts to CONOPS development for specific DPSs and Multi-Service Force Deployment (MSFD) documents, the evaluations of those CONOPS conducted in studies, and alternative concepts developed throughout these processes. Scenario products addressing the "long-term" future provide guidance to the Science and Technology planning community.

Selection of content and assumptions for scenarios to be generated under the Analytic Agenda are guided by strategic and operational issues and priorities identified in official strategic planning documents, including the National Security Strategy (NSS), Quadrennial Defense Review (QDR), and National Defense Strategy (NDS), but particularly the Guidance for the Development of the Force (GDF). For current year analyses, the strategic guidance is derived from the Guidance for the Employment of the Force (GEF). Scenario products and data produced under the Analytic Agenda should provide full coverage of all of the above issues and priorities.

OUSD (P) is responsible for ensuring conformance of the Analytic Agenda scenario set with strategic guidance, and it shares responsibility with OSD (CAPE) and the Joint Staff J-8 in ensuring conformance of study design for joint analyses with priorities identified in strategic guidance.

Additionally, the results of joint analyses conducted under the Analytic Agenda should inform future rounds of strategic planning activities.

APPENDIX C:
POTENTIAL TAXONOMY OF FIELDS

The taxonomy developed for IDA's Open Scenario Repository beta site (http://openscenarios.ida.org/) consists of the classification of the following fields. Because the fields are unique, users can select the fields to search and browse scenarios within the repository. The scenarios in the beta site were reviewed to identify values for each of the fields, if applicable, before being included in the repository. This taxonomy is meant to be a starting point for a taxonomy that may be used for an online open scenario repository and is not exhaustive.

Scenario ID:	The identifier for the scenario is in the repository (e.g., #207).
Scenario Name:	The scenario's formal name (e.g., Project 2020).
Purpose:	The purpose for which the scenario is supposed to be used (e.g., to examine counterterrorism operations).
Date Published:	The date the scenario was published (e.g., 2008).
Scenario Classification:	The classification of the scenario (e.g., U = Unclassified, and U//FOUO = For Official Use Only).
Scenario Hyperlink:	The hyperlink to the scenario.
Sponsor:	The official sponsor of the scenario – if applicable (e.g., United States Air Force, Hudson Institute).
Developer:	The person or organization who wrote or developed the scenario – if applicable (e.g., Office of Naval Intelligence).
Geographic Region:	The area of the world the scenario emphasizes – if applicable (e.g., South America)
Country:	The country or countries examined in the scenario – if applicable (e.g., Turkey).
Timeframe:	The time period the scenario examines (past, present, short term, mid term, long term).
Timeframe Range:	The range of dates the scenario examines (e.g., 2010-2025).
Timeframe Minimum:	The first year of the scenario Timeframe Range (e.g., 2010).
Timeframe Maximum:	The last year of the scenario Timeframe Range (e.g.,

2025).

Intended User:	The person or organization whose activities the scenario is intended to support (e.g., joint warfare community).
Level of Detail:[1]	The amount of detail the scenarios has (e.g., low, medium, high).
File Type:	The type of file the scenario is formatted in (e.g., PDF).
Operations Depicted:[2]	The types of operations that are emphasized in the scenario (e.g., major combat operations, Climate Change Scenario).
Context/Road to War (Background and Timeline):	Indicates whether scenario contains Context/Road to War.
Assumptions:	Indicates whether scenario contains Assumptions.
Threat/Challenge (Red):	Indicates whether scenario contains Threat/Challenge (Red).
Objectives (Blue):	Indicates whether scenario contains Objectives (Blue).
Strategic Concept: (Strategic Level)	Indicates whether scenario contains Strategic Concept (Strategic Level).
Concept of Operations (Operational Level):	Indicates whether scenario contains Strategic Concept (Strategic Level).
Forces Data:	Indicates whether scenario contains Forces Data.

---

[1] Determining how much detail a scenario has for IDA's prototype was a subjective process and no specific set of standards were used. In a more refined online open scenario repository, it would be useful to establish a concrete set of standards that would be applied to determine how to describe the level of detail for a specific scenario.

[2] The Range of Military Operations (ROMO) was used to classify the military operations depicted in scenarios on IDA's prototype. For those scenarios that depicted non-military operations, IDA used other labels that accurately reflected what type of operations were depicted (e.g., civil-military emergency planning).

APPENDIX D
ALLIED AND INTERAGENCY INVOLVEMENT

In Phase One of the Open Scenario Study, IDA received questionnaire responses from, and in some instances interviewed, personnel from the following organizations:

- Department of State (DOS)

- Department of Homeland Security (DHS)

- Department of Energy (DOE)

- Department of Treasury (DOT)

- Department of National Defence (Canada)

- Ministry of Defence (United Kingdom)

- Department of Defense (Australia)

Results distilled from both the interviews and the questionnaire indicated that there is a broad demand for unclassified scenarios from some of DOD's most important interagency organizations and allies. [1]

Because of the responses gathered in Phase One of the Open Scenario study, IDA continued to engage some of DOD's most important interagency partners in Phase Two. In Phase Two, IDA initiated a dialogue with principals from the following agencies:

- National Guard Bureau Strategic Plans and Policy Directorate (J5)

- The Federal Emergency Management Agency's (FEMA) Homeland Security Exercise and Evaluation Program (HSEEP)

- FEMA's Director of the Master Exercise Practitioner Program (MEPP)

- The Exercise Program Director for Ohio Emergency Management Agency

---

[1] *Open Scenario Study, Phase I: Assessment Overview and Results* (IDA Paper P-4326), March 2008, pp. 52-6.

- The Senior Planner for the Volusia County, Florida Division of Emergency Management

- Department of Homeland Security Risk Analysis Division

- Center for Homeland Security and Defense, Naval Postgraduate School

Through interactions with these organizations, IDA gained insight into the need for and use of unclassified scenarios by several non-DOD agencies. Additionally, IDA discerned instances where an online, unclassified scenario repository would offer opportunities for collaboration between DOD and these organizations. These salient examples are listed below.

Department of Homeland Security

Two of the most popular programs using exercises and scenarios within the Homeland Security community are the Homeland Security Exercise and Evaluation Program (HSEEP) and the Lessons Learned Information Sharing System (LLIS). The former is part of and utilized primarily by FEMA, while the latter is located in the Preparedness Directorate of the Office of Grants and Training within DHS. Both utilize repositories that contain information to aid in homeland security-related training and exercise development. As the Phase One report noted that "The scenarios could also be used to determine how to integrate non-governmental agencies and humanitarian assistance relief efforts into military plans or to estimate the number of mass casualties of U.S. citizens".[2] Thus, the approach described in Chapter VI. of this report might further interagency and NGO-related efforts in support of DOD and Homeland Security planning initiatives.

National Guard

The National Guard has been and remains in the forefront of the civil-military nexus. Whether operating under U.S. Code Title 10 (as a Federal force) or U.S. Code Title 32 (under control of the State), the National Guard has played a major role in all areas involving civil-military cooperation. Within the purview of homeland security, the NG considers itself to be both a "first responder" and a primary defender of the homeland.[3] The National Guard, with their civil support teams and robust CBRNE

---

[2] *Open Scenario Study, Phase I, Volume 1: Assessment Overview and Results* (IDA Paper-P 4326), March 2008, p. 53.

[3] Jack Spencer and Larry M. Wortzel, Ph.D., *The Role of the National Guard in Homeland Security*, Heritage Foundation, April 8, 2002.

training regimens, have been preparing for an enhanced role in civil-military operations since the September 11, 2001 attacks. The National Guard is yet another example of a civil-military component that would benefit from and enhance opportunities to access an online unclassified scenario repository.

Department of State

The Department of State (DoS) and related organizations, such as United States Agency for International Development (USAID), routinely work with non-U.S. governments, agencies and entities that do not usually have access to U.S. classified materials. Nonetheless, to the extent that DoS utilizes scenarios and exercises in support of U.S policy objectives, open scenarios provide a tool towards that end. Winning the peace requires a mirror-image set of planning and exercise tools to that of winning wars. As an example, the strategic importance of the Arab-Israeli peace process, as exemplified by the Palestinian issue, cannot be overestimated and has recently been referred to by two ex-Secretaries of State as an"…issue that requires priority attention."[4] The ability to utilize appropriate open source scenarios as a method to encourage discussion and mediation would be an invaluable tool for DoS representatives.

---

[4]   Brent Scowcroft and Zbigniew Brzezinski, "Middle East Priorities for January 21st", *The Washington Post*, November 21, 2008.

APPENDIX E
SUMMARY OF THE U.S. ARMY'S MULTI-LEVEL SCENARIO (MLS) SUB-TASK

A. BACKGROUND

This appendix provides background information on a sub-task performed by IDA under the Open Scenario Study task that examined the U.S. Army's unclassified Multi-Level Scenario (MLS). The IDA sub-study highlights how the U.S. Army develops and uses the MLS to discern valuable Doctrine, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) changes to its current and future force concepts and systems.[1] It also offers IDA's findings and recommendations on future MLS use and applications for the Department of Defense (DoD).[2]

The MLS Study Sub-Task is part of the broader Open Scenario Study. IDA was tasked, on behalf of its DoD sponsors, to explore and answer several research questions regarding the MLS, offer recommendations for improving the existing construct, and assess its applicability to the Joint community.[3] As part of Phase Two of the Open Scenario Study, which has developed and assessed alternatives that may be used to meet the national security community's demand for unclassified scenarios, IDA was tasked with evaluating the U.S. Army's unclassified MLS construct as a potential alternative for satisfying the DoD-wide demand for unclassified scenarios.[4]

B. APPROACH

To complete the MLS sub-task IDA developed a two part methodology aimed at the rigorous collection and distillation of data. The first part included a literature review and extensive interviews with subject matter experts, including a site visit to Fort

---

[1] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, p. 287. Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities.

[2] *Open Scenario Study: U.S. Army's Multi-Level Scenario Sub-Task* (IDA Paper P-4466), by Jason A. Dechant and James S. Thomason et al., Institute for Defense Analyses, July 2009.

[3] Sponsors include Office of the Under Secretary of Defense (CAPE and AT&L) in coordination with the Joint Staff (J8).

[4] Joint Publication 1-02, pp. S-1-2.

Leavenworth, Kansas where the MLS is developed.[5] During this time IDA examined nearly all of the Army's MLS-related literature, which included the MLS 1.0 and MLS 2.0 scenarios, several MLS background and process briefs, U.S. Army Training and Doctrine Command (TRADOC) memos and regulations, and Experimentation to Action Plans (ETAPs) promulgated by Army Battle Labs (ABLs) after major experiments and activities.[6] The second part of the study methodology involved extensive interviews and communication with the Army's primary MLS personnel. This consisted of visiting five user-community Army Battle Labs where analysis, testing, training, and experimentation take place using MLSs.

C. KEY FINDINGS

Analysis of the MLS literature and information obtained from interviews yielded the following five major findings listed below.[7]

1. **The U.S. Army's MLS 1.0 could serve a number of DoD/Joint purposes if the other Services are included in the MLS development process and follow-on analyses.** If all the Services actively participated in the development process of a single unclassified scenario they could strengthen and enrich the product for DoD wide-use. They could incorporate their current or future force concepts, doctrine, and military perspectives into the scenario which could lead to a more robust scenario.

2. **The U.S. Army's MLS 1.0 is used to identify DOTMLPF findings at some of the user-community Battle Labs and it could be strengthened to improve and expand insights.** The battle labs possess the expertise to enrich the baseline unclassified MLS. The battle labs should work closely with the MLS developers to provide them with feedback on the MLS construct to expand the functionality and capability.

---

[5] The U.S. Army's development team consisted of the following: U.S. Army Capabilities Integration Center (ARCIC), U.S. Army Training and Doctrine Command (TRADOC), TRADOC Analysis Center (TRAC), and TRADOC Intelligence Support Activity (TRISA).

[6] The Experimentation to Action Plan (ETAP) is an Army Capabilities Integration Center (ARCIC) directed document that provides the informational linkage from experiment results and recommendations to the office of primary responsibility (OPR) and suggested supporting and coordinating staffs for ensuring implementation of DOTMLPF recommendations. The ETAP sections include: Insights, DOTMLPF Domain Focus, Recommendations, OPR, Supporting Organization, and Recommended Coordination.

[7] *Open Scenario Study: U.S. Army's Multi-Level Scenario Sub-Task* (IDA Paper P-4466), July 2009.

3. **The MLS should be available in an unclassified repository for reuse and wider distribution within the Army.** Army battle labs prefer to use a scenario that their models have already been programmed to use because it saves time and money. In addition, they would be very familiar with the scenario which could allow them to test specific DOTMLPF domains.

4. **The MLS, as it currently stands, should not be certified or endorsed for DoD-wide use until the MLSs are jointly developed for use by all Services.** Pulling together all the stakeholders into the scenario development process could allow for substantive adjustment to future force concepts. The Services could then leverage existing unclassified scenarios to perform testing, experimentation, and analysis.

5. **If the U.S. Army MLS is expanded to include other Services and Joint concepts in the development process, an organization in the modeling and simulation community could provide guidance to elevate the scenario(s) for DoD-wide use.** It would be very helpful to have a cross-cutting management body to provide oversight to the development process and subsequent analysis of unclassified scenarios. The management body must have a broad understanding of the direction DoD is headed, it could establish rules (e.g., access) and scenario criteria for the unclassified set, and determine where best to house the unclassified scenario set (e.g., an online repository).

APPENDIX F
GRAPHS OF POTENTIAL APPROACHES

Major Elements of an Approach

Each element below has defining features/characteristics

Variations and Combinations of These Exist

1. Online Repository: An online, searchable database of unclassified scenarios developed by any available sources.
   - Sample features: accessibility, refresh rate, taxonomy, etc.

2. Certification (of existing scenarios): Designing of pre-existing set of unclassified scenarios as "preferred" for use throughout community.
   - Sample features: Certification body, criteria, standards, etc.

1. Unclassified Scenario Set: Development and maintenance of a new set of unclassified scenarios akin to Defense Planning Scenarios. Examples include National Planning Scenarios and Project Horizon.
   - Sample features: Participation, updating, identifying gaps, etc.

2. Declassification of Classified Scenarios: Identification and removal of sensitive materials in classified scenarios to produce official sanitized unclassified set.

Figure 5. Major Elements of an Approach

Building Viable Approaches

Variations and Combinations of These Exist

Notional Approaches...

1. Online Repository

| Entirely Public | Password Protected | Self-Populating |

Others:
-Refresh rate
-Taxonomy
-Etc..

2. Certification (of existing scenarios)

| Committee Certified | Single Office | Self-Certifying |

Others:
- Criteria
-Standards
-Etc..

3. Unclassified Scenario Set

| Identify Scenario Gaps | Develop New Scenarios | Modify Existing Scenarios |

Others:
- Participation
-Updating
-Etc..

Approach A

| Entirely Public | |
| Community Certified | Develop New Scenarios |

Approach B

| | Password Protected |
| Single Office | Modify Existing Scenarios |

Others...

More or less ambitious variations of each exist

Figure 6. Building Viable Approaches

An Online Repository: The Foundation of an Unclassified Scenario Approach

- Under direction of the sponsor, ***any*** approach designed to meet the demand for unclassified scenarios will include an online repository

- The ***major*** variable of an online repository is ***accessibility.***

- **Four Degrees of Accessibility:**

  1. <u>Open Access:</u> All scenarios are publicly available (e.g. Defenselink.mil/pubs).

  2. <u>Limited Access:</u> Repository users must meet a limited of access standards in order to use the repository (e.g. Modeling and Simulation Resource Repository).

  3. <u>Restricted Access:</u> Repository users must meet a rigorous set of access standards in order to use the repository (e.g. E-Room).

  4. <u>Layered Access:</u> Some scenarios are available to all, while others are limited or restricted.

- The repository's accessibility is a function of how much demand for unclassified scenarios DoD wishes to meet:
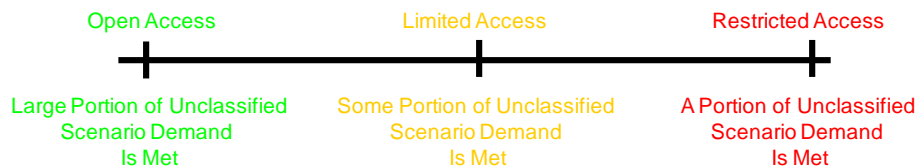
Figure 7. An Online Repository: The Foundation of an Unclassified Scenario

Potential Unclassified Scenario Approaches

- 4 major unclassified scenario approaches exist, each with unique variations

Develop New Scenarios

Certify Existing Scenarios

Combination (4 potential Combos)

Online Repository

Subcomponents
- Boolean/Keyword Search
- Message Board
- Rating System
- Wiki Engine

Subcomponents
- Open Access
- Limited Access
- Restricted Access
- Layered Access

Subcomponents
- Taxonomy of searchable fields
- Standards for scenario inclusion
- Others
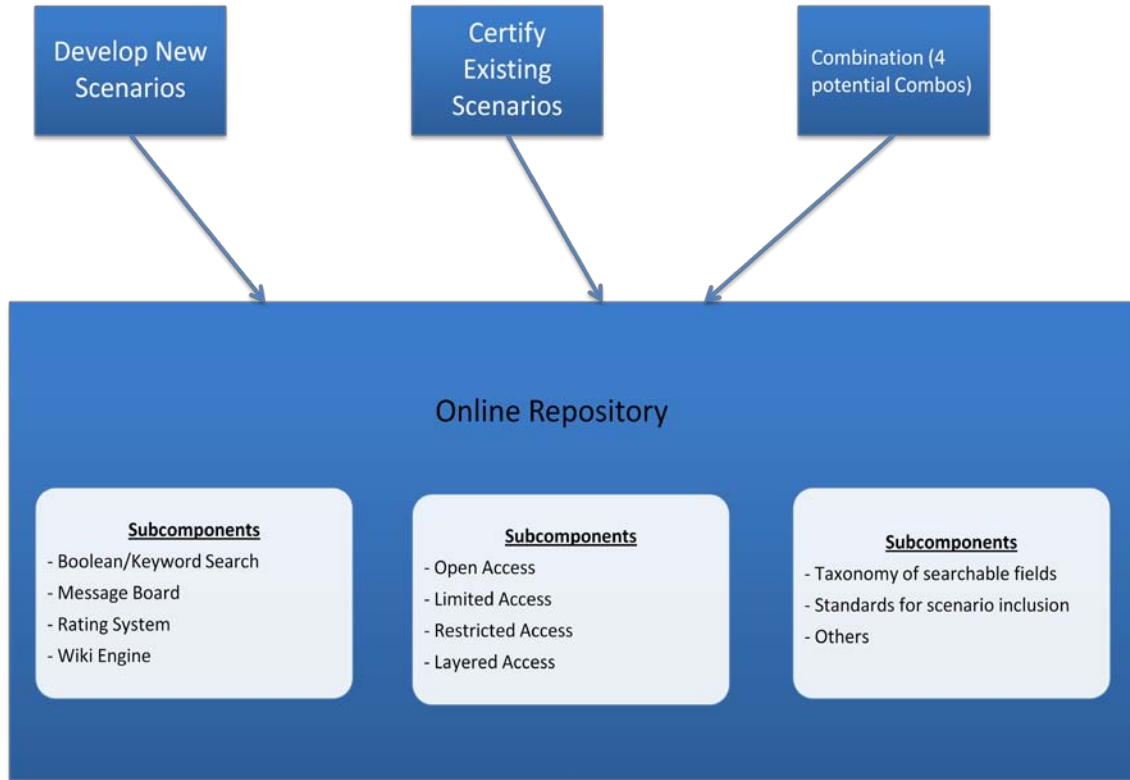
Figure 8. Potential Unclassified Scenario Approaches

Approach #1: Standalone Open Scenario Repository

- A standalone open scenario repository would house or link existing unclassified scenarios in a searchable, online virtual space so that they are accessible to those who need them

Unclassified Scenario Collection Process

Existing Unclassified Scenarios

Online Repository

Subcomponents
- Boolean/Keyword Search
- Message Board
- Rating System
- Wiki Engine

Subcomponents
- Open Access
- Limited Access
- Restricted Access
- Layered Access

Subcomponents
- Taxonomy of searchable fields
- Standards for scenario inclusion
- Others
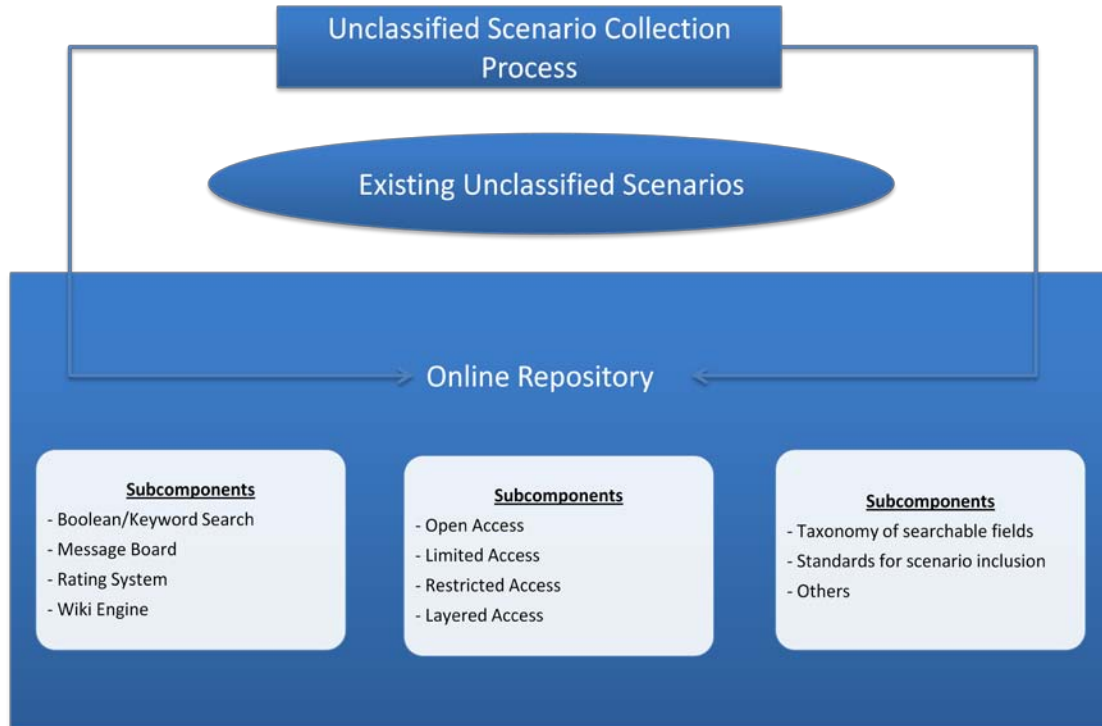
Figure 9. Approach #1: Standalone Open Scenario Repository

Approach #2: House Newly Developed Scenarios in a Repository

Establish an independent unclassified scenario development capacity akin to the DPS process	Leverage the existing DPS enterprise to construct unclassified scenarios	Outsource unclassified scenario development (e.g. commercial firms, FFRDCs, Universities, etc.)	Leverage the value of existing ad hoc unclassified scenario efforts (e.g. COCOMS, Armed Services) and fill in gaps by piggybacking on the existing DPS process.
1. Parallel DPS Process	2. Piggyback Existing DPS Process	3. Outsource Unclassified Scenario Development	4. Distributed Enterprise

Online Repository

Subcomponents
- Boolean/Keyword Search
- Message Board
- Rating System
- Wiki Engine

Subcomponents
- Open Access
- Limited Access
- Restricted Access
- Layered Access

Subcomponents
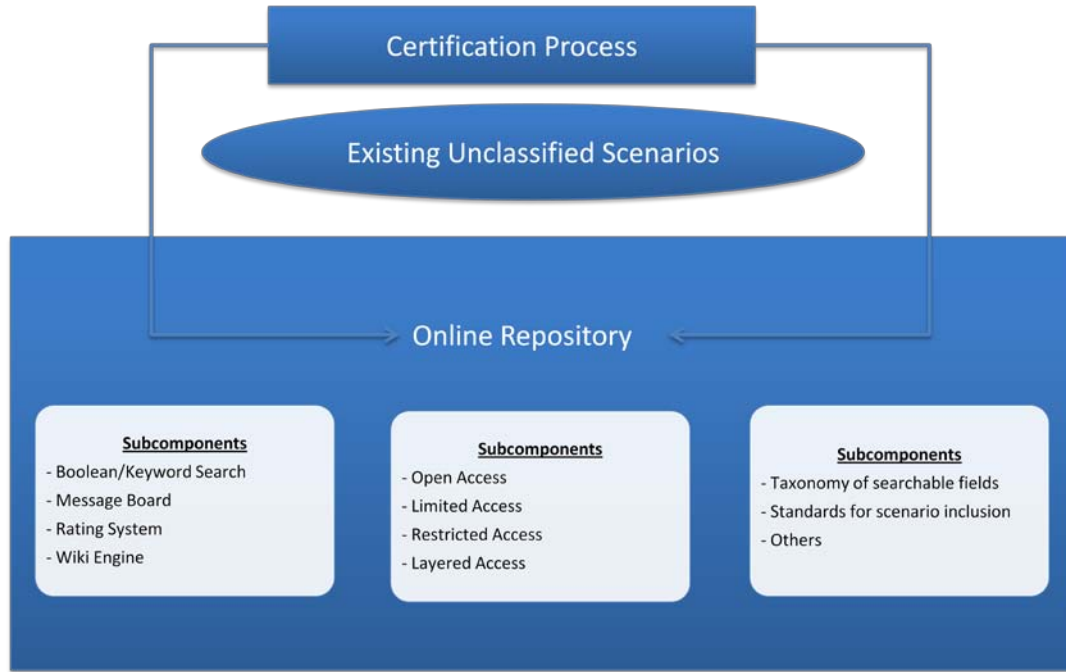- Taxonomy of searchable fields
- Standards for scenario inclusion
- Others

Figure 10. Approach #2: House Newly Developed Scenarios in a Repository

Approach #3: Certify and House Existing Unclassified Scenarios in a Repository

-**Purpose of Certification:**
-Information for Users: Certification could assist users of the repository in sorting or filtering scenarios according to a single set of standards.
-Organizational Preference: certification could represent an officially expressed preference of the certifying organization (e.g. OSD) for a particular set of unclassified scenarios.

Certification Process

Existing Unclassified Scenarios

Online Repository

Subcomponents	**Subcomponents**	**Subcomponents**
- Boolean/Keyword Search	- Open Access	- Taxonomy of searchable fields
- Message Board	- Limited Access	- Standards for scenario inclusion
- Rating System	- Restricted Access	- Others
- Wiki Engine	- Layered Access	

Figure 11. Approach #3: Certify and House Existing Unclassified Scenarios in a Repository

APPENDIX G
TECHNICAL CONSIDERATION FOR DESIGNING THE OPEN SCENARIO REPOSITORY

The ability to provide a repository for unclassified scenarios appears to be a simple task on the surface, but consideration of current and future requirements should be taken into account when deciding on a final system design. Many factors will influence the design of an open scenario repository and should be weighed appropriately.

A. GENERAL DESIGN CONSDIDERATIONS FOR A CLIENT-SERVER ARCHITECTURE

When designing a Web-based server with dynamic content, there are a number of issues that must be considered and questions answered in order to determine what type of server to host the data on. Factors influencing the design will include:

Workload

- How many concurrent users will the server need to support?

- How large is the database estimated to be?

- What repository functions are required?

- Can adequate functionality be provided with a single-tier server or is a multi-tiered design required?

Maintenance

- Who will host the repository?

- Who will build and maintain the server?

- What Operating System (OS) do they support?

- What Relational Data Base Management System (RDBMS) do they support?

- What application/programming languages do they support?

Security

- What are the security requirements?

- Who gives access (level) to the users?

- How are users validated when accessing the repository?

- Who is allowed to post scenarios?

- What restrictions will be placed on the use of the scenarios by the owners?

An Open Scenario Repository can be as simple as a single machine running a web server with a Microsoft Access® database and some simple CGI (Common Gateway Interface) or .ASP[1] scripts to provide the dynamic content, or it may be a complex as a multi-server solution with one server providing the web interface, another providing the application logic (a program used to manipulate the data), and a server running Microsoft SQL Server or Oracle RDBMS.

B. WORKLOAD

The repository workload will depend on the total number of customers, the level of access, the number of simultaneous users, the number of scenarios in the repository, the level of detail of the taxonomy, and whether the actual scenarios are stored in the repository or only links to where the scenarios are stored. The workload will also depend on the features provided by the repository.

Repository Requirements

Proposed features for the Open Scenario Repository include the following:

- Search of scenarios using a taxonomy of fields,

- Web-like search of actual scenarios,

- Download and/or upload of scenarios,

- Blog/message board,

- Rating system message board,

- Wiki engine that would allow user posting of scenarios, feedback, and ratings,

- Software for management of the repository.

Other features that might be considered:

- Handle use of the repository by multiple users with disparate operating systems,

---

[1] ASP.NET is a free technology that allows anyone to create a modern web site.

- Maintain archives of the repository usage.

A commercial interface between the client server and the application server can simplify the tasks handled by the application level. One such interface is the Citrix Metaframe Interface toolkit which facilitates the access control problems and for the most part eliminates the problem of disparate user operating systems by providing a web browser based interface to the repository. This interface also allows the repository to begin to track what the various users are doing with the repository scenarios and will maintain archives of the scenarios. This interface presents the user a menu of options such as accessing message boards, searching the taxonomy, and downloading scenarios.

The size and complexity of the repository will dictate whether a single-tiered or multi-tiered architecture would be preferred. With either type of architecture, the same capabilities must be provided.

Single versus Multi-Tiered Architectures

The difference in server design can be viewed in the simplest terms as being either a single server, running a single web server process that handles all user requests, versus multi-tiered where there are multiple servers each handling different parts of the users' requests.
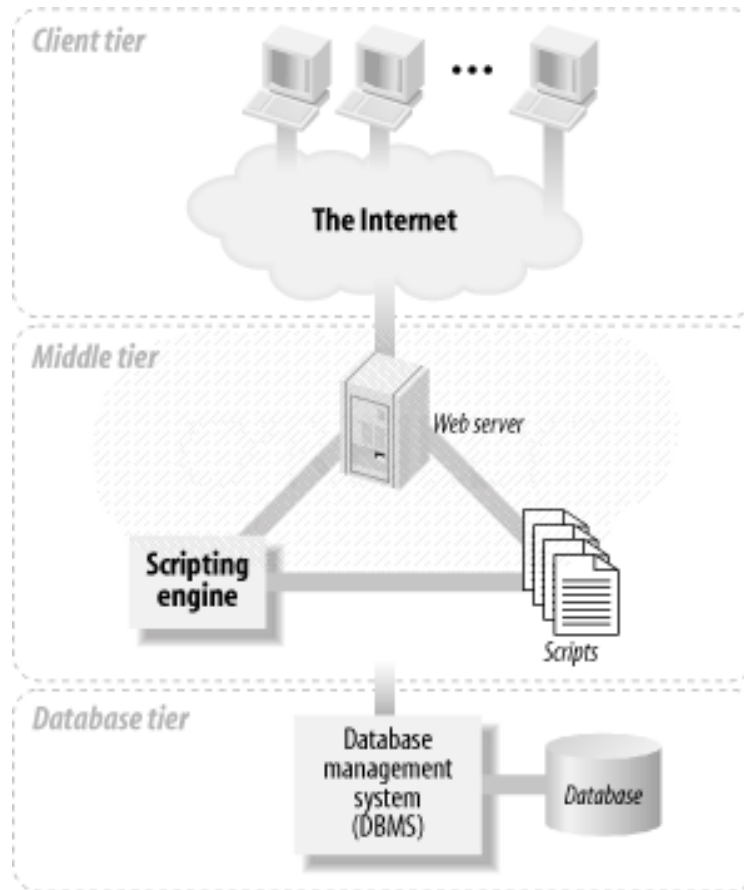
Single-Tiered Client-Server Architecture

A single-tiered architecture consists of a single web server that handles all user requests. The user interface, functional process logic ("business rules"), computer data storage and data access are developed and maintained as one module on one platform.

Multi-Tiered (Three-Tiered) Client-Server Architecture

A three-tiered model is a client-server architecture in which the user interface, functional process logic ("business rules"), computer data storage and data access are developed and maintained as independent software modules, most often on separate platforms.

The three-tier model is considered to be software architecture. Apart from the usual advantages of modular software with well defined interfaces, the three-tier architecture is intended to allow any of the three tiers to be upgraded or replaced independently as requirements or technology change. For example, a change of operating system from Microsoft Windows® to Linux/UNIX would only affect the user interface code.

Typically, the user interface runs on a desktop PC or workstation and uses a standard graphical user interface (GUI), while the functional process logic may consist of one or more separate modules running on a workstation or application server. An RDBMS on a database server or mainframe contains the computer data storage logic. Additionally, the middle tier may be multi-tiered itself (in which case the overall architecture is called an "n-tier architecture").

Figure 12. Three-Tiered Client-Server Architecture

The three-tier architecture has the following tiers:

- **Client or Presentation Tier -** This is the top most level of the application. The presentation tier displays information related to such services as browsing merchandise, purchasing, and shopping cart contents. It communicates with other tiers by outputting results to the browser/client tier and all other tiers in the network.

- **Middle or Application/Logic Tier -** The logic tier is pulled out from the presentation tier and has its own layer. It controls an application's functionality by performing detailed processing.

- **Data or Database Tier -** This tier consists of Database Servers. Here information is stored and retrieved. This tier keeps data neutral and independent from application servers or business logic. Giving data its own tier also improves scalability and performance.

C. MAINTENANCE AND SECURITY

The most important question for maintenance is: who will host the repository? The answer to this question may depend on the following:

- Who is paying for the repository?

- Who might have overall responsibility for making scenarios available?

- Who has the hardware, software and personnel to support the system?

- What level of security is required and can the prospective host provide that security?

The selection of a host may go through several iterations of matching capabilities of prospective host organizations to repository requirements. There may be several design options that will meet the repository requirements and the one that most closely matches the capabilities of a prospective host might be selected. The host does not need to initially possess the hardware and software required for the repository but it needs to be able to incorporate them into its current configuration.

D. SPECIFIC DESIGN DECISIONS FOR THE OPEN SCENARIO REPOSITORY

The following areas need to be carefully thought through in order to obtain a design that will be robust and flexible enough to fulfill the requirements:

What operating system will be used?

Operating System

- Microsoft Windows®

- Linux/UNIX

- Other

What RDBMS will be needed?

- Database engine

- SQL Server (Microsoft)

- 10g/11g (Oracle)

- Mysql (Open Source)

- Other

What application server software will be needed?

- Application Server

- CGI PHP/Perl (Open Source)

- ColdFusion (Adobe)

- OAS Application Server (Oracle)

- ASP (Microsoft)

- Inmagic DB/Textworks

What are the security issues that will be faced?

- Security issues

- Username/Password

- Record level protection

- Certificate

- Access level

E. DETERMINING THE OPEN SCENARIO REPOSITORY WORKLOAD

When designing the Open Scenario Repository, a web server with dynamic content, one must consider how much processing will be required to perform each function in the design. It is important to understand the workload and the capabilities of the machine(s) on which that work will be handled. Understanding the total Open Scenario Repository load will help determine if and how to split the workload across multiple servers.

Critical to a repository's design is a determination of how much data manipulation will take place on the server. Put in simple terms, when a request from a user comes into the server, how much processing will take place from the time the server queries the

database, to the time the results are returned to the user's browser. This will involve any data manipulates and formatting of the data received from the database or other sources.

F. DECIDING ON THE OPERATING SYSTEM

When deciding on the operating system on which to host the services, the following issues must be considered:

- Maintenance

  o Does the organization responsible for providing maintenance on the server have experience with that specific operating system?

- Application server requirements

  o What application server is supported by the operating system?

  o Is the organization responsible for providing maintenance familiar with the application server?

G. DECIDING ON AN RELATIONAL DATABASE MANAGEMENT SYSTEM

There are a number of considerations to take into account when deciding on a database engine to use for an open scenario repository.

- What database functions are required? Triggers? Stored Procedures?

- What operating system will the database engine be running on?

- Will the database be greater than 2 Gigabytes?

- What type of database connection will be utilized?

  o A native connection, Open Data Base Connection (ODBC), Java Database Connectivity (JDBC)?

Database engine considerations will not be too critical due to the fact that most database engines will run on multiple operating systems, but some performance and expandability issues will be relevant in deciding the appropriate RDBMS.

Database Schema

The current database schema contains, among others, the following fields:

No.	Scenario Name	Purpose	Date Published	Developer	Geographic Region	Country	Timeframe	Level of Detail	Operations Depicted

Additional feature enhancements to the service and schema of the repository should be considered by the repository's owners. For instance, the owners may want to consider the date the scenario was added to the repository, and consider adding "Date Added" field to the schema. If the owners are considering row level password protection, meaning each specific scenario has a password associated with it, then they might want to consider adding a password field. Additional fields to consider include:

- Updated date

- Original scenario name

- Who is involved in the scenario

- Type of scenario

  o Strategic

  o Tactical

  o Economic

  o Other

H. DECIDING ON AN APPLICATION SERVER

A determination must be made as to what application server, if any, is required to perform the necessary functions on the server to provide the desired repository capabilities. The application server may be the same computer as the web server or it may be separate from the web server. The application server operates between the client and the database.

In addition to program development and serving web pages to clients, application servers address the following issues, which include deployment issues:

- Scalability - Involves capacity management, allowing increasing user demand to be met and managed efficiently. The server may supply performance information allowing administrators to change the configuration to enhance performance for increased demand.

- Database connectivity - Efficient data flow - The application server can manage the requests to the database server along with caching requests for the same data when appropriate, thereby relieving and managing some of the load on the database server.

- Programming language support - A sophisticated application development environment with or without application to HyperText Markup Language (HTML) integration may be offered.

- Security - There may be requirements to secure or encrypt information between the client and the server.

To understand what the application server does, consider the following model for a dynamic HTML web server. Typical web servers provide static content that has been programmed previously. A dynamic HTML web server provides this content on demand, typically based on some user input.

There are a number of different methods and tools that are available to implement an application server:

- CGI PHP/Perl (Other Open Source software)

- ColdFusion (Adobe)

- OAS Application Server (Oracle)

- .ASP/.NET (Microsoft)

- Inmagic DB/textworks

I. DECIDING ON THE SECURITY REQUIREMENTS

A determination must be made as to what level of security is required, i.e., what granularity of security will be provided on this server. Is it sufficient to require that a user only have a generic username and password to logon to the server, or should there be the capability to control who sees what and who can do what?

For instance:

- Is there a requirement for multiple levels of password protection for different scenarios?

- Do the repository owners want to allow anyone to view a scenario and only allow specific user with a password to be able to post modified or new scenarios?

- Do the repository owners need to require a user to provide a Public Key Infrastructure (PKI) certificate in order to post to the repository?

- How will the level of access be distributed among users?

J. ADDITIONAL FACTORS INFLUENCING DESIGN

This appendix has touched on the main aspects of factors that need to be addressed in the design of a system. There are other considerations that will be used in determining the design.

Maintenance Costs

The questions that have been addressed in prior chapters of this report and in this appendix will have a great impact not only on the design and implementation phases of the project, but also on the maintenance costs. The trade-offs are sometimes hard to estimate in the initial design phase, but will have a lasting effect on the upkeep and maintenance of the service.

If commercial application server packages are chosen, then the repository's owners can realistically assume that there will be a yearly maintenance fee on the order of 10-20% of the original cost. However, if the owners choose to use open source software, there is only the cost of installing bug fixes and updates. Cost trade-offs usually come with the ease of use with a commercial product versus the low cost of open source/free software.

Application Maintenance

In addition to the maintenance cost of the software itself, there is the maintenance cost for upkeep of the data and the application code. Careful design considerations need to be made when it comes to the software used (open source vs. commercial) and the entity that will be maintaining the software once it is goes to production. If the shop that is going to provide the on-going maintenance and upkeep is a Microsoft shop, for example, and the repository owners have decided to user open source software, then the software might be neglected and become unusable.

K. CONCLUSION

The review of what functions an open scenario repository might have in order to provide the query, modification, and posting of scenarios leads one to believe that a simple single-tied, dynamic-content web server can be set up and configured with basic tools. These basic tools would include ASP.NET scripting and a basic Microsoft Access® database. This does not exclude the possibility of incorporating this simple functionality into an existing infrastructure that is much more complex and expandable.

L. GLOSSARY

This section lists technical terms and software products mentioned in this appendix. Many of the descriptions are taken from web sites that support these products and are documented by footnotes.

- 10g/11g (Oracle) – an Oracle RDBMS.

- .ASP (Microsoft) – ASP.NET from Microsoft is a free technology that allows anyone to create a modern web site.[2]

- CGI – The Common Gateway Interface, or CGI, is a set of standards that define how information is exchanged between the web server and a custom script.

- CGI – CGI is one method by which a web server can obtain data from (or send data to) databases, documents, and other programs, and present that data to viewers via the web.[3]

- Citrix toolkit – facilitates the access control problems and for the most part eliminates the problem of disparate user operating systems by providing a web browser based interface to the repository. This also allows the repository to begin to track what the various users are doing with the repository scenarios.[4]

- ColdFusion (Adobe) – Adobe® ColdFusion® 9 software enables developers to rapidly build enterprise-ready Internet applications by condensing complex business logic into fewer lines of code.[5]

- HTML – Hyper Text Markup Language, which is the predominant markup language for web pages.[6]

- Inmagic DB/Textworks – Inmagic® DB/TextWorks® is a special combination of database and text retrieval software that enables you to build

---

[2] Microsoft ASP.NET website at http://www.asp.net/. Accessed January 28, 2010.

[3] *CGI Programming 101: Learn CGI Today* website at http://www.cgi101.com/learn/. Accessed January 28, 2010.

[4] Citrix Systems website at http://www.citrix.com. Accessed on January 28, 2010.

[5] Adobe ColdFusion website at http://www.adobe.com/products/coldfusion/. Accessed January 28, 2010.

[6] *Wikipedia, The Free Encyclopedia* website at http://en.wikipedia.org/wiki/HTML. Accessed January 28, 2010.

networked and standalone textbases to manage diverse types of information including documents, images, and multimedia.[7]

- JDBC - The Java Database Connectivity (JDBC) application programming interface (API) is the industry standard for database-independent connectivity between the Java programming language and a wide range of databases – SQL databases and other tabular data sources, such as spreadsheets or flat files. The JDBC API provides a call-level API for SQL-based database access.[8]

- Linex/UNIX – a free Unix-type operating system originally created by Linus Torvalds with the assistance of developers around the world.[9]

- Ms Windows® – Microsoft Windows operating system for personal computers

- MySQL (Open Source) - the most reliable, secure and up-to-date version of the world's most popular open source database[10]

- OAS Application Server (Oracle) - Oracle Application Server (OAS) is Oracle's enterprise web platform. While OAS performs all the functions of a normal web server, its main advantage is its tight integration with a backend Oracle database.[11] http://www.php.net/

- ODBC – Open Database Connectivity (ODBC) provides a standard software API method for using database management systems (DBMS). The designers of ODBC aimed to make it independent of programming languages, database systems, and operating systems.[12]

- OS – operating system

- PC – personal computer

---

7 InMagic DB/Text Library website at http://www.inmagic.com/products/LibrarySuite/index.html. Accessed January 28, 2010.

8 Oracle Sun Developer Network: JAVA SE Technologies – Database website at http://java.sun.com/javase/technologies/database/. Accessed January 28, 2010.

9 Linux Online website at http://www.linux.org/. Accessed January 28, 2010.

10 MySQL Enterprise Frequently Asked Questions website at http://www.mysql.com/products/enterprise/faq.html#1. Accessed January 28, 2010.

11 *Chapter 4, Oracle Application Server (OAS), Oracle Web Applications* website at http://docstore.mik.ua/orelly/oracle/webapp/ch04_01.htm. Accessed on January 28, 2010.

12 *Wikipedia, The Free Encyclopedia* website at http://en.wikipedia.org/wiki/Open_Database_Connectivity.   Accessed on January 28, 2010.

- Perl - Perl is a programming language developed by Larry Wall, especially designed for processing text. It stands for Practical Extraction and Report Language.[13]

- PHP – PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. [14]

- PKI certificate - A PKI certificate, which stands for Public Key Infrastructure certificate, allows someone to combine their digital signature with a public key and something that identifies them, an example being their real life name. This certificate is used to allow computer users to show that they do own the public keys they claim to. In other words, it is a security mechanism for public keys.[15]

- RDBMS – Relational Data Base Management System

- SQL – sequential query language

- SQL Server (Microsoft) - SQL Server 2008 provides a scalable business intelligence platform optimized for data integration, reporting, and analysis, enabling organizations to deliver intelligence where users want it.[16]

- Wiki - A wiki is a website that allows the easy creation and editing of any number of interlinked Web pages, using a simplified markup language or a What You See Is What You Get (WYSIWYG) text editor, within the browser. Wikis are typically powered by wiki software. Wikis are often used to create collaborative websites, to power community websites, for personal note taking, in corporate intranets, and in knowledge management systems.[17]

---

[13] PERL Tutorials Point website at http://www.tutorialspoint.com/perl/index.htm. Accessed January 28, 2010.

[14] PHP Hypertext Preprocessor website at http://www.php.net/. Accessed January 28, 2010.

[15] TopBits.com PKI Certificate website at http://www.tech-faq.com/pki-certificate.shtml . Accessed January 28, 2010.

[16] Microsoft SQL Server 2008 website at http://www.microsoft.com/sqlserver/2008/en/us/overview.aspx. Accessed January 28, 2010.

[17] *Wikipedia, The Free Encyclopedia* website at http://en.wikipedia.org/wiki/Wiki. Accessed January 28, 2010.

APPENDIX H
GLOSSARY

ABL	Army Battle Labs
ARCIC	Army Capabilities Integration Center
CAC	common access card
CAPE	Cost Assessment and Program Evaluation
CBA	Capabilities-Based Assessment
CBRNE	Chemical Biological Radiological Nuclear (High) Explosives
CC-2	Conventional Conflict
CD	compact disc
CGI	common gateway interface
COCOM	Combatant Command
COMSEC	communications security
CONOPS	concept of operations
CWG	community working group
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOS	Department of State
DOT	Department of Treasury
DOT&E	Office of the Director, Operational Test and Evaluation Directorate

DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
DPS	Defense Planning Scenarios
DTIC	Defense Technical Information Center
ETAP	Experimentation to Action Plan
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
FOUO	For Official Use Only
GDF	Guidance for the Development of the Force
GEF	Guidance for the Employment of the Force
GUI	graphical user interface
HSEEP	Homeland Security Exercise and Evaluation Program
HTML	hypertext markup language
IDA	Institute for Defense Analyses
IS	information system
JDBC	Java Date Base Connectivity
JCIDS	Joint Capabilities Integration and Development System
JDS	Joint Data Support
JFCOM	U.S. Joint Forces Command
LES	Law Enforcement Sensitive
LLISS	Lessons Learned Information Sharing System
MEPP	Master Exercise Practitioner Program
MLS	multi-level scenario
M&S IPT	Modeling and Simulation Integrated Process Team
MSFD	Multi-Service Force Deployments
MSRR	Modeling and Simulation Resource Repository
NDS	National Defense Strategy

NG	National Guard
NGO	non-governmental organizations
NSS	National Security Strategy
ODBC	Open Data Base Connectivity
OPR	office of primary responsibility
OPSEC	operations security
OS	operating system
OSD	Office of the Secretary of Defense
OUSD (AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
OUSD (CAPE)	Office of the Under Secretary of Defense for Cost Assessment & Program Evaluation
OUSD (I)	Office of the Under Secretary of Defense for Intelligence
OASD NII	Office of the Assistant Secretary of Defense for Networks and Information Integration
OUSD(P)	Office of the Under Secretary of Defense for Policy
OUSD (P&R)	Office of the Under Secretary of Defense for Personnel & Readiness
PC	personal computer
PKI	Public Key Infrastructure
PPBES	Planning, Programming, Budgeting, and Execution System
QDR	Quadrennial Defense Review
RDBMS	Relational Data Base Management System
ROMO	range of military operations
SBU	Sensitive But Unclassified
S/CRS	Office of the Coordinator for Reconstruction and Stabilization
SSSP/ISP	Steady State Security Posture/Integrated Security Posture
TRADOC	U.S. Army Training and Doctrine Command

TRISA	TRADOC Intelligence Support Activity
USAID	United States Agency for International Development
USG	United States Government
WYSIWYG	what you see is what you get

APPENDIX I
REFERENCES

Cuba, Daniel L., Michael F. Fitzsimmons, John T. Hanley, Jr., James H. Kurtz, Lance M. Roark, Vincent P. Roske, Jr. *Improving Integration of Department of Defense Processes for Capabilities Development Planning.* IDA Paper P-4154. Alexandria, VA: Institute for Defense Analyses, September 2006.

Dechant, Jason A., James S. Thomason, Michael F. Niles, Zachary S. Rabold. *Open Scenario Study, Phase One, Vol I: Assessment Overview and Results.* IDA Paper P-4326. Alexandria, VA: Institute for Defense Analyses, March 2008.

Dechant, Jason A., Anthony C. Hermes, Zachary S. Rabold, James S. Thomason. *Open Scenario Study; U.S. Army's Multi-Level Sub-task.* IDA Paper P-4466. Alexandria, VA: Institute for Defense Analyses, July 2009.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington D.C.: Joint Doctrine Division, J-7, Joint Staff., 12 April 2001, as amended through 31 October.

Scowcroft, Brent and Zbigniew Brzezinski. "Middle East Priorities for January 21st." *The Washington Post*, November 21, 2008.

Spencer, Jack and Larry M. Wortzel, Ph.D. *The Role of the National Guard in Homeland Security.* Washington D.C.: Heritage Foundation, April 8, 2002.

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
January 2010	Final	

4. TITLE AND SUBTITLE

Open Scenario Study, Phase Two Report: Assessment and Development of Approaches for Satisfying Unclassified Scenario Needs

5a. CONTRACT NO.

DASW01-04-C-0003

5b. GRANT NO.

5c. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)

Jason A. Dechant, James S. Thomason, Ylli Bajraktari, Mary Catherine Flythe, Anthony C. Hermes, Nicholas S. J. Karvonides, Michael F. Niles, Zachary S. Rabold, Robert T. Raffel, Contributor: Rachael D. Dubin

5d. PROJECT NO.

5e. TASK NO.

AK-6-2841

5f. WORK UNIT NO.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NO.
IDA Paper P-4537

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Director, Study and Analytic Support Division
OSD Cost Assessment and Program Evaluation
1800 Defense Pentagon, Room 3C117
Washington, DC 20301-1800

10. SPONSOR'S / MONITOR'S ACRONYM(S)

11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report, titled *Open Scenario Study, Phase Two Report: Assessment and Development of Approaches for Satisfying Unclassified Scenario Needs* explores elements of an approach that may be used to satisfy the national security community's demand for unclassified scenarios. In this report, the Institute for Defense Analyses (IDA) explores four major elements that any Department of Defense (DoD) approach to meeting unclassified scenario demand could include: 1) an online open scenario repository, 2) the certification of existing unclassified scenarios, 3) development of new unclassified scenarios, and 4) the declassification of classified scenarios. IDA examines each of these elements independently and in combination and ultimately concludes that the national security community's demand for unclassified scenarios could best be met by using variations of several of the elements in combination with one another. This report also highlights major findings from Phase Two of IDA's Open Scenario Study and offers the a recommended approach for better addressing the need for unclassified scenarios.

15. SUBJECT TERMS

unclassified scenarios; open scenarios; scenarios; open scenario repository; open scenario database; unclassified scenario repository; unclassified scenario database; open scenario demand, unclassified scenario demand, IDA open scenario study, IDA unclassified scenario study

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU	132	19b. TELEPHONE NUMBER (Include Area Code)
U	U	U			